4910-13

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 107 and 139

[Docket No. 28979; Notice No. 97-13]

RIN 2120--AD-46

Airport Security

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of Proposed Rulemaking (NPRM).

SUMMARY: This notice proposes to amend the existing airport security rules. It would revise certain applicability provisions, definitions, and terms; reorganize these rules into subparts containing related requirements; and incorporate some requirements already implemented in airport security programs. This proposed revision also would incorporate certain new measures that would provide for better security. Specifically, this proposal would more clearly define the areas of the airport in which security interests are the most critical and where security measures should be the most stringent. It would modify access control requirements by allowing secondary access media, modify escort procedures for individuals without access authority, and expand the requirement for an identification system to include a challenge system. Further, it would clarify the following: training requirements for airport security personnel; the role of the airport security coordinator; procedures for airport operators to comply with Federal Aviation Administration security directives; procedures for responding to and evaluating threats; and the need to review and test security contingency plans. The intent of this proposal is to enhance security for the

traveling public, air carriers, and persons employed by or conducting business at public airports by increasing awareness of and compliance with civil aviation security measures.

DATES: Comments must be submitted on or before December 1, 1997..

ADDRESSES: Comments on this proposed rulemaking should be mailed or delivered, in triplicate, to: Federal Aviation Administration, Office of the Chief Counsel, Attention: Rules Docket (AGC-10), Room 915-G, Docket No. 28979, 800 Independence Ave., SW., Washington, DC 20591. Comments may also be sent electronically to the following internet address: 9-NPRM-CMTS@faa.dot.gov. Comments may be examined in Room 915-G between 8:30 a.m. and 5 p.m. weekdays, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: Office of Civil Aviation Security Policy and Planning, Civil Aviation Security Division (ACP-100), Penny Anderson Federal Aviation Administration, 800 Independence Ave. SW., Washington, DC 20591; telephone (202) .267-3418

SUPPLEMENTARY INFORMATION:

Comments Invited

Interested persons are invited to participate in this rulemaking by submitting such written data, views, or arguments as they may desire. Comments relating to the environmental, energy, federalism, or economic impact that might result from adopting the proposals in this document are also invited. Substantive comments should be accompanied by cost estimates. Comments

should identify the regulatory docket or notice number and should be submitted in triplicate to the Rules Docket (see ADDRESSES). All comments received, as well as a report summarizing each substantive public contact with FAA personnel on this rulemaking, will be filed in the docket. The docket is available for public inspection before and after the comment closing date. All comments received on or before the closing date will be considered by the the Administrator before taking action on this proposed rulemaking. Late-filed comments will be considered to the extent practicable. The proposals contained in this document may be changed in light of comments received. Comments received on this proposal will be available, both before and after the closing date for comments in the Rules Docket for examination by interested persons. However, the Assistant Administrator for Civil Aviation Security has determined that the airport security programs required by part 107 contain sensitive security information. As such, the availability of information pertaining to airport security programs is governed by 14 CFR Part 191 (Withholding Security Information from Disclosure Under the Air Transportation Security Act of 1974).

Commenters wishing the FAA to acknowledge receipt of their comments must include a self-addressed, stamped postcard on which the following statement is made: "Comments to Docket No. 28979." The postcard will be date-stamped and mailed to the commenter.

Availability of NPRM

Any person may obtain a copy of this NPRM by submitting a request to the Federal Aviation Administration, Office of Rulemaking, ARM-1, 800 Independence Ave., SW.,

Washington, DC 20591, or by calling (202) 267-9677. Communications must identify the notice number of this NPRM.

An electronic copy of this document may be downloaded using a modem and suitable communications software from the FAA regulations section of the Fedworld electronic bulletin board service (telephone: 703-321-3339) or the Office of the Federal Register's electronic bulletin board service (telephone: 202-512-1661). Internet users may reach the FAA's webpage at http://www.faa.gov or the Office of the Federal Register's webpage at http://www.access.gpo.gov/su_docs for access to recently published rulemaking documents.Persons interested in being placed on the mailing list for future NPRM's should request from the above office a copy of Advisory Circular No. 11-2A, Notice of Proposed Rulemaking Distribution System, which describes the application procedure.

Background

This proposed rule was written before the tragic crash of TWA 800 on July 17, 1996. That accident raised concerns about the safety and security of civil aviation, leading the President to create the White House Commission on Aviation Safety and Security, headed by the Vice President. The Commission issued an initial report on September 9, 1996, with 20 specific recommendations for improving security. On February 12, 1997, the Commission issued its Final Report with 57 recommendations, 31 of which deal with improving security for travelers. In addition, the Federal Aviation Reauthorization Act of 1996 (Pub. L. 104-264) was signed on October 9, 1996, and directs the FAA to amend rules to upgrade civil aviation security.

The FAA is working to respond to the recommendations of the Commission and to carry out the legislation, and has issued several proposals. On March 11, 1997, an Advance Notice of Proposed Rulemaking on the certification of screening companies was issued (62 FR 12724, March 17, 1997), and on March 14, 1997, the FAA issued a Notice of Proposed Rulemaking on employment history; verification and criminal records checks (62 FR 13262, March 19, 1997)..

The rules proposed in this notice were not written in response to .the Commission or the Reauthorization Act. However, this notice, which proposes to update the overall regulatory structure for airport and air carrier security, is the result of a multi-year effort involving the FAA, airports and air carriers, and the Aviation Security Advisory Committee. The extensive proposed revisions are considered to be consistent with the intentions of the mandates, contain proposals that industry has identified as necessary or appropriate, and outline a new organization for the regulations that would assist in developing future changes to the rules. For these reasons, the FAA is publishing this proposed rule for comment. The FAA anticipates that any final rule based on this proposal will incorporate responses to these mandates.

Terrorist Incidents

In response to a rise of hijacking incidents, and to ensure the security of airports serving scheduled air carriers, the Federal Aviation Administration (FAA) issued 14 Code of Federal Regulations (CFR) part 107 on March 18, 1972. The rule required each airport operator to implement prescribed security measures by developing and observing an airport-specific security program. Part 107 has been amended on several occasions, but the rule has never undergone a comprehensive update.

Since the inception of part 107, the primary threat to civil aviation has expanded beyond hijacking to bombing of aircraft and murderous attacks within airports. The following incidents are indicative of this evolution:

- December 27, 1985: Simultaneous attacks at two European airports against the general public in open terminal areas. At least 13 people were killed and approximately 80 wounded at Rome's Leonardo da Vinci International Airport; 4 persons were killed and approximately 45 wounded at Vienna's Schwechat International Airport.

- September 5, 1986: Terrorist assault on Pan American (Pan Am) Flight 73. Four terrorists assaulted Flight 73 in Karachi, Pakistan as the aircraft waited to take off. The four terrorists were dressed similarly to airport security personnel and drove a van resembling an airport security vehicle alongside the aircraft. The terrorists stormed the aircraft and after 17 hours of negotiations, the aircraft's auxiliary power unit failed. Anticipating an attack by security forces, the terrorists opened fire on the massed passengers, killing 22 persons and injuring 125 others before security forces could intervene.

- September 14, 1986: The bombing of an international terminal building. A device detonated in a trash can located in front of the international terminal building of the Kimpo International Airport, Seoul, South Korea. Five persons were killed and 29 were injured.

- November 11, 1987: Explosives detonated in a passenger terminal. Explosives in baggage detonated, possibly prematurely, in the passenger terminal of the Beirut International Airport, Beirut, Lebanon. Six persons were killed and 73 were injured. No person(s) claimed responsibility; however, the person carrying the bag was killed.

- December 21, 1988: The bombing of Pan Am Flight 103. All 243 passengers and 16 crew on board, plus 11 persons on the ground at Lockerbie, Scotland, were killed. Subsequent inspection of the reconstructed aircraft determined that a device consisting of plastic explosives inside a tape cassette player was responsible for the destruction of Flight 103. The device had been concealed in checked luggage. Individuals working for the Government of Libya are responsible for the bombing. One conspirator was the former manager of the Libyan Arab Airlines (LAA) office in Valletta, Malta and retained full access to the airport. Using this access privilege and other knowledge gained as representatives of LAA, the conspirators bypassed security checks at Valletta's Luqa Airport and inserted the suitcase containing the bomb into baggage of an Air Malta flight to Frankfurt.

- August 26, 1992: Explosive device placed in an international terminal. A 20-pound explosive device was placed in the international terminal in the Houari Boumedienne International Airport, Algiers, Algeria. Twelve persons were killed and 126 were injured. Members of the Islamic Salvation Front were arrested. Their intent was to disrupt foreign involvement in Algeria.

- November 3, 1994: Armed individuals seized the airport. Armed militant Muslim activists seized the Saidu Sharif Airport in Pakistan's Northwest Frontier Province and barricaded the runway. Pakistani paramilitary forces attacked several days later. Five persons were killed and at least 17 were injured.

- December 24, 1994: Hijacking and possible intention to destroy Air France flight 8969. While on the ground at Houari Boumedienne International Airport, Algeria, Air France Flight 8969 was commandeered by four terrorists armed with automatic weapons, hand grenades, and explosives. The four gunmen wore what appeared to be Air Algerie uniforms and displayed airport identification. The hijackers killed three people. French counterterrorism forces stormed the aircraft at Marignane Airport in Marseille, France; all four hijackers were killed. Explosives were found on the aircraft, leading to speculation that the hijackers intended to blow up the aircraft over Paris.

- July 22, 1996: A bomb detonated in a public area of a terminal building. Six persons were killed and an estimated 60 others were injured when a bomb exploded in the concourse outside of the departure/arrival lounges at the Lahore International Airport, Lahore, Pakistan. The device, containing approximately 3 kilograms of explosives, reportedly had been left in a briefcase and placed beneath a bench near the domestic departure lounge. The explosion occurred moments before the departure of PIA flight 715 for Karachi. There were no immediate claims for the bombing.

Fifty-nine attacks have been recorded at airports throughout the world during the past 5 years. These attacks have included 24 bombings; 15 attempted bombings; and 20 shootings, shellings (such as mortar attacks), arsons, and similar incidents. At least 41 persons have been killed and more than 250 injured in attacks at airports between 1992 and 1996.[1]

Terrorism has been, for the most part, a phenomenon afflicting U.S. interests overseas, and the threat to U.S. civil aviation is assessed to be higher abroad than it is domestically. The World Trade Center bombing in February 1993, however, indicates that terrorism is also a very real threat in the United States, and may be on the rise.

Ramzi Ahmed Yousef has been convicted for the bombing of Philippine Airline flight 434 (December 11, 1994) and for conspiring to bomb U.S.-flag aircraft. Authorities believe that Yousef and his co-conspirators acted on their own volition, in opposition to U.S. foreign policy in the Middle East, and that they were assisted by local radical sympathizers in the Philippines and the United States. Their conspiracies are indicative of an emerging trend in terrorism, characterized by terrorist elements operating without traditional organizational structure or state sponsorship.

The Federal Bureau of Investigation (FBI) characterizes such terrorists as seeking a "common political, social, economic, or personal objective which transcends nation-state boundaries." The U.S. Department of State, commenting on global terrorism trends notes that "terrorism by extremist individuals or groups claiming to act for religious motives" continue to dominate international terrorism. [2]

---

1 Criminal Acts Against Civil Aviation: 1996, US Department of Transportation, Federal Aviation Administration, Office of Civil Aviation Security.

2 For further analysis of the terrorist threat, please refer to the following public documents: Terrorism in the United States: 1994, U.S. Department of Justice, Federal Bureau of

The number of international terrorist attacks against US interests fell between 1995 and 1996, although incidents involving American targets still represented more than 24% of the total attacks worldwide in 1996. Domestically, the FBI asserts that the U.S. is not immune to international terrorism, describing the terrorist threat as "real and potentially lethal." The FAA views these developments as cause for concern.[3]

In addition, individual acts of revenge or criminality must be considered since the consequences of such acts can be just as deadly. Following are three examples:

- December 7, 1987: Destruction of Pacific Southwest Airlines (PSA) Flight 1771. Flight 1771 crashed when a recently terminated airline employee boarded the Los Angeles - San Francisco flight with a handgun, shot one passenger (his former supervisor), the flightcrew, flight attendant, and presumably himself. As a result, all 38 passengers and five crew on board were killed. The fired employee retained his airline identification after his dismissal and used it to bypass the passenger screening checkpoint.

- August 14, 1990: Gunman gained unauthorized access at Washington National Airport. A man armed with a .38 caliber revolver entered the Ogden Allied Services garage at Washington, D.C.'s National Airport, and held several employees at gunpoint. He was a former employee at Ogden and had voluntarily left his job. He commandeered a fuel truck, forced an Ogden employee to drive onto the air operations area and fired

---

Investigation

3 Patterns of Global Terrorism: 1995, U.S. Department of State, April 1996.
Patterns of Global Terrorism: 1996, U.S. Department of State, April 1997.

several shots at a second Ogden fuel truck, wounding two persons. He was in possession of 30 to 40 rounds of ammunition when he was arrested. A molotov cocktail was recovered from the commandeered fuel truck, and several others were found in the gunman's vehicle.

- May 7, 1995: Gunman exchanged fire with police at Minneapolis/St. Paul International Airport. A man armed with a 7.62 mm Norinco SK5 assault rifle attempted to enter a secured area through a door in the baggage claim area. Unable to gain access, the gunman fired several rounds, shattering panes of plate glass, and then proceeded through the terminal firing his weapon. The gunman then exited the terminal to a public driveway, exchanged fire with responding police officers and was shot three times before being apprehended. Three persons were injured by flying debris, but none seriously. The weapon used appeared to have been altered to fire automatically and the gunman was in possession of 90 rounds of ammunition. The gunman never gained access to the sterile or secured areas of the airport.

- October 13, 1995: A low-level explosive device destroyed an automated facility serving La Guardia International Airport. The facility, a Low Level Windshear Alert System (LLWAS), is located in a remote area near Flushing Airport, formerly a general aviation field. The LLWAS is housed in a metal box on a utility pole and is surrounded by a perimeter fence that was cut to gain entry. Even though the LLWAS was not fully functional for several days, air traffic to La Guardia was not jeopardized. An arrest was made in this matter. Despite an anti-

government leaflet found at the scene, no connection was found between the person arrested and right-wing terrorist organizations.

Response to Terrorist Incidents

The incidents discussed above have led to concerted efforts to strengthen aviation security around the world and particularly to strengthen security at U.S. airports. The FAA responded by issuing emergency amendments to airport security programs, using part 107 authority.

The destruction of Pan Am Flight 103 resulted in numerous changes to civil aviation security. The Presidential Commission on Aviation Security and Terrorism was critical of the domestic U.S. civil aviation security system for failing to provide the proper level of protection for the traveling public and urged major reforms. Specifically, the commission recommended that the "FAA initiate immediately the planning and analysis necessary to phase additional security measures into the domestic system over time."[4] The Commission's report prompted the Aviation Security Improvement Act of 1990 (Public Law 101-604), enacted November 16, 1990.

The new law mandated many changes to airport and air carrier security programs, as well as Federal staffing and reporting procedures. Several rulemakings were initiated to impose hiring standards for air crew and security personnel, and training standards and criminal history checks for certain airport and air carrier personnel. The act also required the FAA to coordinate with the FBI to assess the domestic air transport system, develop security guidelines for airport design and construction, and expand the security technology research and development program.

---

4 President's Commission on Aviation Security and Terrorism, Report to the President, May 15, 1990.

The proposed revisions to part 107 also respond to two other Federal reports. In September 1993, the Office of the Inspector General (IG) of the U.S. Department of Transportation issued a report critical of certain aspects of the FAA's oversight of airport security systems.[5] In January 1994, the General Accounting Office (GAO) issued a report suggesting further actions the FAA could take to improve civil aviation security.[6]

The IG report found significant deficiencies in the effectiveness of access control and challenge procedures at five U.S. airports. The report recommended that airport and air carrier implementation of procedures for access control and challenge be strengthened, stressing that the FAA must take steps to increase airport and air carrier employees' awareness and responsibility for those procedures.

In January of 1994, the FAA responded to the report by meeting with representatives of airports, air carriers and other airport tenants, and employee groups/unions to discuss the IG's findings and to emphasize the need for improved employee security awareness. Simultaneously, the FAA began focused inspections at U.S. airports with the highest volume and most complex security operations. Slated to continue on a routine basis, these special inspections targeted the security measures that the IG found to be a universal weakness - access control and challenge procedures.

The response has been an industry-wide commitment to address the identified weaknesses and improve compliance. In particular, many airports and air carriers have improved their training programs and instituted programs to provide individual incentives for compliance and

---

5 DOT Office of Inspector General, Audit of Airport Security, Federal Aviation Administration, Report No. R9-FA-3-105, September 20, 1993.

6 United States General Accounting Office, Report to Congressional Committees, Aviation Security: Additional Actions Needed to Meet Domestic and International Changes, January 1994.

escalating disciplinary action for instances of non-compliance. Compliance at airports which have instituted such programs has improved markedly. The FAA proposes to implement similar measures at other part 107 airports by clarifying and modifying access control, identification display, and challenge requirements.

Separately, the GAO issued a report entitled "Aviation Security - Additional Actions Needed to Meet Domestic and International Challenges," in response to a Congressional inquiry on FAA's efforts to implement the Aviation Security Improvement Act of 1990. GAO found that the FAA has taken important steps in response to the act and cited additional actions that should be taken to enhance the FAA's security programs and initiatives. These actions include - (1) pilot-testing new procedures before implementation, (2) strengthening human factors research and its application, (3) making systematic analytical use of information that the FAA collects during air carrier and airport security inspections, and (4) providing airport security coordinators with security clearances, so that they can be given classified information regarding threats to civil aviation.

Similar to the IG report, the GAO report highlighted the need for the FAA to increase industry employees' overall awareness of security measures. The report concluded that the FAA must refine security training and procedures to increase personnel sensitivity to security requirements. The FAA agrees that complacency must be combated, and as previously noted, considers improved employee training and increased accountability to be an essential part of the solution.

Specific responses to issues raised in the IG and GAO reports are discussed below in the "Section by Section Analysis."

The Role of the Aviation Security Advisory Committee

The Department of Transportation and the FAA are convinced that the aviation industry and general public should have input into the development of future aviation security measures and issues. On April 3, 1989, the Secretary of Transportation announced the formation of a national aviation security advisory committee under the provision of the Federal Advisory Committee Act (Title 5 U.S. Code, Appendix II).

The Aviation Security Advisory Committee (ASAC) was formed to examine all areas of civil aviation security and to ensure a higher degree of safety for the traveling public by recommending improvement of aviation security equipment and procedures. The ASAC is chaired by the FAA's Assistant Administrator for Civil Aviation Security and makes recommendations to the FAA Administrator. Committee membership represents a balance of Federal government, aviation industry, and consumer advocacy groups, including:

1. Air Courier Conference of America
2. Air Line Pilots Association International
3. Air Transport Association of America
4. Aircraft Owners and Pilots Association
5. Airport Law Enforcement Agencies Network
6. Airports Council International, Inc.
7. Allied Pilots Association
8. American Association of Airport Executives
9. Association of Flight Attendants
10. Aviation Consumer Action Project
11.. Aviation Security Contractors Association

12 Cargo Airline Association

13. Families of Pan Am 103 Lockerbie

14.. International Airline Passengers Association

15. National Air Carrier Association, Inc.

16. National Air Transportation Association

17. Regional Airline Association

18. U.S. Department of Defense (Policy Board on Federal Aviation)

19. U.S. Department of Justice (Federal Bureau of Investigation)

20. U.S. Department of State

21. U.S. Department of Transportation (Office of Intelligence and Security and Federal Aviation Administration Technical Center)

22. U.S. Department of the Treasury (Customs Service, Immigration and Naturalization Service, and Secret Service)

23. U.S. Postal Service

24. Victims of PanAm Flight 103

All ASAC meetings are open to the public and are announced in the Federal Register. Meetings are typically held three times a year. Members of the public are permitted to attend and appear before the committee, subject to reasonable limitations of space and time.

The FAA invited the ASAC to comment on the underlying issues and potential solutions associated with the revision of parts 107 and 108. In December 1993, the FAA sought the ASAC's input on a "discussion paper" that presented a broad scope of security issues and

concerns. A copy of this paper is filed in the FAA public docket for this Notice of Proposed Rulemaking (NPRM).

To address the issues raised in the discussion paper, the ASAC formed two subcommittees to develop recommendations on airport and air carrier security issues, respectively, and provided the FAA formal recommendations on March 15, 1994. Individual ASAC members also provided comments on issues when their respective organizations differed from the position taken by the committee. The views of the ASAC and of individual committee members were then forwarded to the FAA with an overall recommendation that security regulations should remain flexible and contain only general security performance standards. Specific recommendations are addressed individually in the "Section-by-Section Analysis."

Discussion of the Proposed Rule

This proposed revision of part 107 would comprehensively update airport security regulations to more efficiently and effectively address terrorist and other criminal threats to civil aviation. This proposed action would incorporate both procedures currently in airport security programs and new security procedures, in a manner that is intended to allow regulated entities and individuals to understand their responsibilities more readily. When a final rule has been adopted, the FAA will update relevant advisory circulars and prepare a standard airport security program that will contain specific security measures that are considered sensitive under part 191 and therefore cannot be included in the proposed revision. Lastly, the proposed revision would incorporate certain new measures that would provide for better security. For example, the proposed revisions make individuals directly accountable to the FAA for violating certain regulations and would require airports to include in their security programs specific disciplinary

action and penalties to be taken with employees or tenants that do not comply with security requirements. Through these changes, the FAA hopes to create a more effective mixture of individual and corporate responsibility for complying with security regulations, particularly those relating to access controls and challenge procedures.

Air carrier security programs required by part 108 also have been amended extensively since 1985. The FAA proposes to revise part 108, which governs aircraft operator security, concurrently with this part. The rulemakings will proceed in tandem. All references to proposed part 108 in this preamble are intended to refer to the concurrently proposed revision of part 108. Further, this proposal would modify the airport emergency plan required under 14 CFR part 139, the certification and operations rules for land airports, to indicate that the evaluation of threats would be handled under airport security programs.

The proposed revisions of part 107 and part 108 represent a comprehensive approach toward upgrading the security requirements of the civil aviation system. The intent of these proposed revisions is to foster consistency and standardization throughout the national civil aviation security program. Where possible, the revisions of part 107 and part 108 propose nearly identical language to enhance, clarify, or propose security measures for implementation by both airport operators and air carriers.

Changes to definitions in proposed § 107.3 and § 108.3 are intended to promote a common understanding within the aviation community when used in these respective regulations. Moreover, the proposed definitions for both parts 107 and 108 take into account the need to clarify the division of responsibility between air carriers and airport operators for the implementation of aviation security measures.

Proposed § 107.7 and § 108.5 would clarify the authority of the Administrator to conduct inspections or tests to determine air carrier compliance with 49 U.S.C. Subtitle VII, and the regulations, and the airport operator's and air carrier's obligation to provide FAA Special Agents the necessary access and identification medium to conduct inspections.

Both proposals include language, in proposed § 107.9 and § 108.7, that would prohibit persons from knowingly making false statements or entries on security-related documentation. Proposed § 107.11 and § 108.9 contain language that would prohibit persons from interfering with or compromising required security methods or procedures. Further, new language proposed in § 107.103(a) and § 108.103 would require the inclusion of a security compliance program within an airport operator's and air carrier's security program.

Proposed § 107.105 and § 108.105 reflect similar procedural language for the approval and amendment of security programs. Proposed § 107.209 and § 108.223 would require the airport operators and air carriers to establish accountability standards for identification media.

Finally, language is proposed in both notices to expand training requirements to include personnel performing security-related duties (proposed § 107.211 and § 108.227), to incorporate similar sections for the implementation of contingency plans (proposed § 107.301 and § 108.307), and to require compliance with Security Directives (proposed § 107.303 and § 108.305).

Section-by-Section Analysis

In this notice, the FAA proposes to revise existing §§ 107.1 through 107.31. The FAA further proposes to add several new sections, some of which address the security responsibilities of persons and the requirements for personnel identification systems. Individual airport security

programs which implement the requirements of part 107 would be subject to revision as a consequence of this rulemaking (see the section below entitled "Implementation Schedule").

Historically, part 107 has been amended in increments with each amendment being added to the regulation at the end of the part. The FAA proposes to reorganize the regulation into specific subparts identified by subject matter. To do so would require a change in the current numbering scheme. For example, all sections that specify security program content and approval process would be listed in proposed subpart B, entitled "Security Program." All sections which describe the operational aspects of systems or procedures required in the approved security program would be listed in proposed subpart C, "Operations," and so on.

This arrangement of the sections by subpart is intended to make part 107 "user friendly" by allowing the reader to locate a particular section easily and to identify all requirements relevant to a specific subject readily. Arranging the regulation by subparts also would allow the FAA to keep similar sections together rather than to add serially to the body of the regulation.

Throughout the proposed rule, references are made to 49 U.S.C. Subtitle VII. This statute is the recodification of FAA's authority to prescribe aviation security regulations previously found in the Federal Aviation Act of 1958, 49 U.S.C. App. 1301 et seq.

Subpart A - General.

Section 107.1 Applicability

This notice proposes to extend the applicability of existing § 107.1. This proposal would extend the applicability to employees, contractors, and other individuals who have significant security responsibilities at an airport and whose actions could diminish the effectiveness of those

systems, methods, or procedures required by this part, by acts such as subverting an access control system, divulging security-sensitive information, or falsifying records.

Further, the FAA proposes to extend airport security requirements beyond airports serving scheduled passenger operations. Instead, the proposed requirements would apply to an airport regularly serving any air carrier required to have a security program under parts 108 and 129. This is not intended, however, to imply that an airport which only serves an occasional single air carrier flight is necessarily required to implement an airport security program. Title 49 U.S.C. 44903 specifies that the FAA shall impose certain security requirements on airports "regularly serving" air carrier operations.

This notice also proposes to move existing § 107.1(a)(3), which applies the requirements of this part to persons entering a sterile area, to part 108. This change would consolidate most security requirements applicable to the sterile area in part 108, since the responsibility for ensuring the integrity of the sterile area rests mainly with air carriers.

Part 107 currently refers to the "Director of Civil Aviation Security " as the official who oversees civil aviation security operations and approves airport security programs. Under internal FAA reorganization, the current title of this position is Associate Administrator for Civil Aviation Security; however, 49 U.S.C. 44932 refers to this official as the Assistant Administrator for Civil Aviation Security. Therefore, paragraph (b) of this section would use the title “Assistant Administrator for Civil Aviation Security.” The FAA intends to resolve this inconsistency before issuance of the final rule. In addition, paragraph (b) would clarify that the Deputy Assistant Administrator for Civil Aviation Security, or any individual formally designated, could act in the capacity of the Assistant Administrator and the duties of this position could be further delegated.

Section 107.3 Definitions

This proposed section would replace existing § 107.3, Security program. The provisions of existing § 107.3 would be incorporated under proposed Subpart B, Airport Security Program. This proposed section also would revise the definitions contained under current § 107.1, Applicability and definitions. The introductory text of this proposed section would make the definitions in proposed part 108 apply to this part.

The term "air operations area" in existing § 107.1 would be replaced by the term "restricted operations area" and its definition modified. The definition "exclusive area" in existing § 107.1 would be revised and grouped with a newly defined "exclusive area agreement." This new definition would ensure clarity of standards pertaining to security agreements between the airports and air carriers or foreign air carriers, and expand the applicability of exclusive area agreements to include not only air carrier leaseholds but individual access points as well. The definitions "escort" and "sterile area" would remain essentially unchanged from existing § 107.1. The definition "escort" would be revised to include reference to the proposed critical security area and restricted operations area; the definition "sterile area" would be revised to clarify the responsibility to conduct inspections of persons and property.

The following definitions would be added: Airport security program, Airport tenant, Airport tenant security program, Assistant Administrator, Critical security area, Exclusive area agreement, Restricted operations area, and Unescorted access authority.

The definitions "airport tenant" and "airport tenant security program" would be added to this section to clarify proposed § 107.113 and to eliminate confusion between airport tenant security programs (which do not apply to air carriers and foreign air carriers that have security programs)

and exclusive area agreements (which only apply to air carriers and foreign air carriers that have security programs).

This notice proposes two new security area definitions. The definition of "critical security area" is introduced for the purposes of proposed § 107.201, Security of the Critical Security Area. The term "critical security area" would be added to replace the term "secured area" found in existing § 107.14. The definition "restricted operations area" would be added to replace the term "air operations area" found in existing §§ 107.1 and 107.13. This definition would be added for the purposes of proposed § 107.203, Security of the Restricted Operations Area. (See below for further discussion of these particular sections).

The description of the intended parameters of "critical security area" and "restricted operations areas" would be purposely limited. Due to the different physical layouts and tenant activities, it is impossible to define with specificity in this proposed rule the boundaries of the proposed critical security area and restricted operations area. As such, the proposed definitions give only general descriptions for critical security area and a restricted operations area.

The term "unescorted access authority" would be defined in this section to support access and identification requirements of the newly proposed critical security area and restricted operations area. It would be included to ensure a clear distinction between individuals that are authorized access and those who are not.

§ 107.5 Airport Security Coordinator

Under this proposal, existing § 107.5 entitled "Approval of security program" would be incorporated into proposed § 107.105 entitled "Approval and amendments," under proposed

Subpart B, Airport Security Program. Existing § 107.29 entitled “Airport Security Coordinator” would be revised and renumbered as new § 107.5 under new Subpart A, General.

As part of the employment standards rulemaking [56 FR 41412; August 20, 1991] adopted in response to the Aviation Security Improvement Act, the FAA Administrator requires airport operators to designate an official at each airport as the airport security coordinator (ASC), to serve as the point of contact with the FAA on security matters and to provide oversight to the airport's security system. The ASC serves as the counterpart of the air carrier's ground security coordinator required under part 108.

To promote standardization, this proposed section would further define the functions and responsibilities of the ASC, including the designation of alternate ASCs. Specifically, the ASC would be responsible for immediately initiating corrective action for each instance of noncompliance and for reviewing all security-related functions for compliance and effectiveness. The proposal also would clarify that an individual serving as an ASC may perform other duties in addition to those required by the FAA, and need not serve full-time as the ASC.

Existing language specifies that the ASC is the airport operator's primary FAA contact, charged with reviewing all security-related functions for compliance with this part and the airport security program. Nevertheless, the ASAC commented that the FAA has not applied this requirement as written, as the ASC is not treated as the FAA's primary contact. Proposed language is intended to clarify the relationship between the FAA and the ASC.

The FAA also proposes to require training for the ASC every 2 years. This training is intended to ensure that ASCs and their alternates remain updated on both airport and air carrier security regulatory and operational requirements. The ASAC opposed inclusion in the rule of any ASC training requirements as well as a description of the ASC's job duties and

responsibilities. The committee did note, however, that, if training is required, credit should be given for the ASC's previous experience.

The FAA therefore requests comments on methods airport operators would use to meet this training requirement. For example, should the FAA require in security programs specific training as it does for air carrier ground security coordinators? Should the training be performed once or should it be recurrent? Should the FAA develop specific guidance or a curriculum for such a training program? How should experience be factored into the training requirement? Should existing ASCs be "grandfathered" under the training requirement?

The FAA also proposes moving to this section certain provisions of existing § 107.31 recently effective [60 FR 51854; October 3, 1995] regarding the ASC responsibility to review and control results of access investigations and to serve as the contact for individuals appealing their results. This change is intended to ensure that all ASC responsibilities are located in the same section of the rule.

§ 107.7 Inspection authority

Under this proposal, existing § 107.7 entitled "Changed conditions affecting security" would be moved to proposed Subpart B, § 107.107. Existing § 107.27 entitled "Evidence of compliance" would be given a new title, "Inspection authority," and revised and renumbered as new § 107.7 under new Subpart A, General. This proposed section would combine the evidence of compliance requirements of existing § 107.27 with the FAA's statutory authority to conduct inspections, investigations, and tests.

Paragraph (a) proposes to state the Administrator's authority to conduct inspections and investigations necessary to determine compliance with part 107 and the security program. The

authority for the FAA to conduct inspections necessary to gauge compliance with Federally-mandated security requirements has, on occasion, been challenged by airport operators. The new language would resolve any misunderstanding regarding the FAA's authority to conduct such inspections under 49 U.S.C. Subtitle VII.

Proposed paragraph (b) would restate the language of existing § 107.27. Proposed paragraph (c) would clarify the airport operator's obligation to provide FAA Special Agents the necessary access and identification media to conduct inspections. This proposed requirement would not be extended in the rule to any FAA employee other than Special Agents. Special Agents are those FAA employees who are authorized to conduct inspections of airport and air carrier security operations and who must possess and present valid FAA-issued credentials. There are some inspections and investigations that a Special Agent can accomplish only with unescorted access to the critical security area and restricted operations area, and it is essential that they be able to accomplish these tasks. The FAA will provide criteria for ascertaining the validity of Special Agents' credentials in non-regulatory guidance materials.

The inclusion of paragraph (c) is intended to facilitate FAA Special Agents conducting inspections, investigations, tests, and other duties without being hampered. It is not intended to allow FAA Special Agents to have access to the entire airport, only to those portions necessary to conduct their duties. Nor is the FAA proposing to require airport operators to give access and identification media to all FAA inspectors. However, as mentioned in the discussion of § 107.209 (d) below, airports may be required to accept FAA form 8000-39 as a valid identification media.

§ 107.9 Falsification

Under this proposal, existing § 107.9 entitled "Amendment of security program by airport operator" would be moved to proposed Subpart B under § 107.105 and retitled "Approval and amendments." Proposed § 107.9 would be new, retitled "Falsification," and would be included under proposed Subpart A, General. This section is the same as the current §107.2 adopted on November 27, 1996 (61 FR 64242 (December 3, 1996).

§ 107.11 Security responsibilities of persons

Under this proposal, existing § 107.11 entitled "Amendment of security program by FAA" would be moved to proposed Subpart B under § 107.105 "Approval and amendments." Proposed § 107.11, retitled "Security responsibilities of persons," would be included under Subpart A, General, and would be completely new.

The FAA believes that the contribution of individuals to the success of the civil aviation security system cannot be overestimated and that the regulations must address the responsibility of individuals who work within the security system. Therefore, the FAA is proposing to prohibit persons from tampering, compromising, or modifying any security system, or carrying a deadly or dangerous weapon, explosive, or destructive substance into sterile areas, critical security areas, or restricted operations areas. Although the airport operator is primarily responsible for carrying out statutory and regulatory security responsibilities under this part, the FAA believes that it is critical that persons employed directly by the airport operator understand the importance of their responsibilities to ensure that security measures within the civil aviation system are properly implemented. It is also important that other persons who may have an impact on aviation security understand their responsibilities.

This section proposes specific requirements to make persons accountable for complying with regulatory prohibitions against interfering with or compromising security methods or procedures required under this part. Moreover, by including these prohibitions in the regulation, this proposed section would permit the use of civil penalty action as a means to gain compliance under this part by persons who are employed by the airport operator and other persons not under the direct authority of the airport operator (such as trespassers).

While there are some instances in which enforcement action against persons may be taken by the FAA, in many cases enforcement action would not be appropriate or necessary. The FAA intends, in proposed § 107.103, to require the airport operator to include in its security program procedures to ensure that persons with unescorted access to critical security areas or restricted operations areas will comply with the requirements of this section. Many airports already have such programs in place and have established penalties, such as monetary fines and revocation of access authorization. The airport operator would remain the primary party responsible for violations, including those committed by their employees and contractors. However, in appropriate cases, persons who fail to comply would be subject to FAA enforcement action, such as a civil penalty of up to $1, 000 per violation of these rules.

The term “person,” used throughout this new section and the proposed rule, is used as defined in 14 CFR Part 1, under § 1.1, General Definitions, which defines person to mean an individual, firm, partnership, corporation, company, association, joint-stock association, or governmental entity, and includes a trustee, receiver, assignee, or similar representative of any of them.

Proposed paragraph (a) of this new section would prohibit tampering or interfering with an airport’s security system, including circumventing access control systems and misusing

identification media. This proposed paragraph is intended to provide a deterrent which, in turn, would promote the effectiveness of the security control measures required by this part.

For instance, many airports have invested in personnel identification systems as a means of satisfying the requirement to control movement under existing § 107.13 (proposed § 107.203). This proposal would require the use of personnel identification systems in both critical security areas and restricted operations areas and would set forth minimum standards for personnel identification systems. Establishing sanctions for not complying with personnel identification media display requirements would significantly promote the effectiveness of personnel identification systems.

Further, this section would prohibit persons from compromising, or rendering less effective, any system implemented in response to the various requirements of this part. This prohibition includes similar language found in existing § 107.25(f) that prohibits the use of an airport-approved identification by any person unless it is issued to that person. However, the proposed language would expand the prohibition to encompass any type of intentional misuse, such as tampering, compromise, or modification, of security systems or the unauthorized circumvention of these systems. Such acts would include writing on walls or doors combination lock numbers that provide access to critical security areas or restricted operations areas, temporarily or permanently disabling electronic access systems, and loaning of access or identification media which would provide access to, or movement within, security-sensitive areas of an airport without authorization.

Under part 108, the responsibility rests with the air carrier for ensuring that unauthorized items which may be harmful to civil aviation or to the traveling public do not get into the sterile area. The FAA, accordingly, believes that the current prohibition found in existing § 107.21 (a)

against the introduction of a deadly or dangerous weapon, explosive, or incendiary into sterile areas is more appropriately located in part 108. The FAA proposes transferring the existing prohibition found in § 107.21 (a) to proposed part 108.

The risk to the traveling public presented by the presence of a deadly or dangerous weapon, explosive, or incendiary, or destructive substance should not be underestimated. Paragraph (b) of this section, as proposed, has been drafted to prohibit the unauthorized possession of such weapons or other dangerous items in sterile areas, critical security areas, and restricted operations areas. The current rules refer to the carriage of "explosive, incendiary, or deadly or dangerous weapons" in various places, including existing § 107.21 and § 108.9. The statute, however, refers to searching persons and property for the presence of a "dangerous weapon, explosive, or other destructive substance." (See 49 U.S.C. 44902) In order to make more clear what items the air carriers search for and what items are controlled in various areas secured for the purposes of part 107, the FAA proposes to refer throughout the revised part to "deadly or dangerous weapon, explosive, incendiary, or other destructive substance." This change is proposed in paragraph (b) of this section as well as proposed § 107.101(a)(1), § 107.219(c)(1), and § 107.219(c)(4)(ii). The FAA also will provide guidance on destructive substances.

This section is also intended to prohibit persons from conducting unauthorized "tests" of airport security systems by compromising or circumventing any element of the system. However, proposed paragraph (c), would allow for individuals authorized by the Federal government, airport operator, and air carrier to conduct tests and inspections of security systems.

Provisions regarding the carriage of firearms by law enforcement officers and other authorized personnel found in existing § 107.21(b) would be included in proposed paragraph (d). Paragraph (d) proposes that provisions of this section that apply to firearms and weapons would

not be applicable to law enforcement personnel, Federal Air Marshals, and certain individuals authorized in an airport security program to carry a weapon.. This paragraph would further exempt persons properly transporting declared firearms under proposed § 108.213 or hazardous materials under 49 CFR part 175 from firearms and weapons prohibitions. Proposed paragraph (d)(7) also would exclude from these prohibitions weapons and firearms legally carried aboard non-air-carrier aircraft, such as general aviation pilots operating personal aircraft and transporting firearms in compliance with state and local laws.

The concept of requiring persons to be responsible for complying with security measures was generally supported by the ASAC, particularly the airport operator representatives. Two ASAC members, the Air Line Pilots Association and the National Air Transport Association, however, expressed reservations about the feasibility of enforcing such a requirement and suggested that security resources could be better used elsewhere to achieve the same results. By promoting awareness of security responsibilities, this proposal also would address the concerns raised by the DOT Inspector General about employee awareness of, and compliance with, access control and challenge procedures. Further, this proposed section parallels efforts to require that persons be accountable for their actions related to the dissemination of sensitive security information [Sensitive Security Information, final rule published 62 FR 13736, March 21, 1997].

Other federal regulations and statutes may also contain applicable security and safety responsibilities of persons, including the following: proposed § 107.207, Access investigation; proposed § 108.201 Screening of persons and property and acceptance of cargo; proposed § 108.213 of this part, Carriage of weapons; Part 191 of this chapter,

;Protection of Sensitive Security Information; 49 CFR part 175, Transportation of hazardous materials; 49 U.S.C. 46302, regarding false information involving aircraft piracy, interference with flight crew members, carrying a weapon, and other criminal laws; and 49 U.S.C. 46303, regarding carriage of a weapon.

Subpart B - Airport security program.

§ 107.101 General requirements

While part 107 is a public document and sets forth broad airport security requirements, the security-sensitive details of how an airport meets these requirements are contained separately in the airport's FAA-approved, non-public security program. The FAA intends to continue to use this method and proposes a new security program requirements section, § 107.101. This proposed section would be included under proposed Subpart B which would incorporate all sections relating to airport security programs. The provisions of existing § 107.3 (a) would be stated in this proposed section. The FAA believes that this minor change will help the reader comprehend the overall purpose and format of an airport security program.

This new section would incorporate similar provisions of the existing regulation that require the airport security program to be in writing, and that a copy be kept at the airport operations office. The program's objective has been modified to include protection against the introduction of a deadly or dangerous weapon, explosive, incendiary, or other destructive substances onto aircraft. Also, the reference to the Director of Civil Aviation Security would be updated to Assistant Administrator and reference to part 191 prohibitions on the distribution and disclosure of sensitive security information would be included.

The FAA is developing aStandard Airport Security Program (SASP) to aid airport operators in developing and revising their security programs. Drafting of the model program is being coordinated with the revision of part 107 and it is scheduled to be available shortly after the publication of the final rule of part 107. Additionally, the FAA is revising security advisory circulars to ensure that they reflect any changes to part 107 resulting from this rulemaking; the circulars are intended to be available references for the development and revision of airport security programs.

§ 107.103 Content

This proposed section would be new and would be added to proposed Subpart B, Airport Security Program. It would describe the required content of airport security programs. Basically, it would revise the provisions of existing § 107.3.

Existing § 107.3 defines the type of air carrier operation that requires a specific airport security program. Currently, the type of security program an airport operator must implement is expressed in terms of the type of aircraft operations. The proposed revision would express the applicability in terms of aircraft operations regulated under proposed § 108.101. Proposed § 108.101, Security program: Adoption and Implementation, requires each air carrier to adopt and carry out a security program as it applies to the type of operations conducted. This change is intended to promote consistency and interdependency between parts 107 and 108.

The FAA designs security regulations to provide varying levels of protection based upon the size, type, and frequency of aircraft operations. Security provisions, therefore, are more demanding at airports where air carriers utilize large transport airplanes with 60 seats or more, and have scheduled departures and arrivals. The number and nature of crimes against civil

aviation since 1972 validates the connection between the requirement for an airport security program and the type of aircraft serving a given airport.

Experience shows that airports served only by smaller aircraft need not comply with all requirements appropriate for airports served by larger aircraft. This approach currently allows smaller airports to implement security measures in a more economical manner. The FAA believes that this has provided an acceptable level of security at such facilities and proposes to continue this approach to airport operator security programs.

The proposed rule continues to specify three different security programs varying in complexity, but the proposed part 108 would modify the type of passenger operations that would determine the program required. The most comprehensive security program would continue to be applicable to airports serviced by scheduled passenger operations with aircraft of more than 60 seats.

The type of passenger operations that trigger the two remaining types of airport security programs have been expanded somewhat, as the result of proposed changes to part 108, to ensure complete protection of the sterile area and to ensure security of all passengers, even those enplaned by private charters and on helicopters (discussed below).

As proposed, airports that serve scheduled passenger or public charter passenger operations with aircraft having a passenger seating configuration of more than 60 seats would continue to have in their security program descriptions of the following:

1. Areas to be secured and those adjacent to the airport that would affect security;
2. Procedures to control access to areas to be secured;
3. Exclusive areas and the procedures each air carrier must use to notify the airport operator when that air carrier cannot adequately control access;

4. Law enforcement support and training;
5. System for maintaining records; and
6. Alternate security procedures to be used in emergencies and other unusual conditions.

Proposed § 107.103 (a) also would add new requirements to require such airports to include in their security program a description of the following:

1. Airport security coordinator's duties, means of contact, training and identification;
2. Security compliance program;
3. Critical security area boundaries, activities, entities and signs, as well as procedures, facilities, and equipment used to perform the control functions;
4. Restricted operations area boundaries, activities, entities and signs, as well as procedures, facilities, and equipment used to perform the control functions;
5. Sterile area boundaries and procedures, facilities and equipment used to control access, other than the passenger screening checkpoint;
6. Personnel background check procedures;
7. Personnel and vehicle identification systems;
8. Escort and challenge procedures;
9. Employee and tenant training programs;
10. Schedule for submitting records;
11. Procedures, facilities, and equipment supporting air carrier passenger screening operations, including law enforcement support;
12. Procedures, facilities, and equipment supporting the contingency plan;

13. Procedures for handling Security Directives, Information Circulars, and classified information, as appropriate;

14. Procedures for public advisories;

15. Incident management procedures; and

16. Each airport tenant security agreement, including a description of the area and procedures, facilities, and equipment used to perform the control functions, and methods by which the airport operator will monitor and audit the tenant.

A second level of standards, contained in proposed § 107.103(b), would be required for airport operators serving air carrier operations described in proposed § 108.101(a)(2) and (a)(3) and existing § 129.25(b)(2) and (b)(3). Existing § 107.3(g) requires an airport operator to have a security program if served by scheduled passenger or public charter operations where passengers are enplaned from, or deplaned into, a sterile area. Proposed § 107.103(b) would still require an airport serving these type of air carrier operations to have an airport security program but, by referencing proposed § 108.101(a)(2) and (a)(3), these operations would be expanded to also cover public charter operations using aircraft with less than 61 seats and any private charter operations when passengers are enplaned from, or deplaned into, a sterile area.

For such airports, the minimum law enforcement standards would remain essentially the same; however, requirements for an airport security coordinator, as well as the establishment of contingency plans and incident response procedures, are proposed. As these additions typically are procedural in nature, the FAA believes that the inclusion of such requirements would not unduly burden airports with such limited operations. Instead, this enhancement would promote

better compliance and emergency preparedness by ensuring better coordination and dissemination of security-related information, and response to threats to civil aviation.

Specifically, this notice proposes that an airport operator serving air carrier operations specified in proposed § 108.101(a)(2) and (a)(3) and existing § 129.25(b)(2) and (b)(3) would continue to have in their security program the descriptions of law enforcement support and training, the descriptions of a system for maintaining records, and also the identity and means to contact the airport security coordinator.

Proposed § 107.103 (b) also would require such airports to include in their security program a description of the following:

1. Airport security coordinator duties and training;
2. Schedule for submitting records;
3. Procedures, facilities, and equipment supporting the contingency plan;
4. Procedures for handling Security Directives, Information Circulars, and classified information, as appropriate;
5. Procedures for public advisories; and
6. Incident management procedures.

The third and final level in proposed § 107.103(c) is intended for airports served by air carriers required to have a security program under proposed § 108.101 (a) (4) and existing § 129.25(b)(4). Similar to existing § 107.3(f), an airport security program would be required if the airport is served by air carriers that have scheduled passenger operations in an aircraft with a passenger seating configuration of more than 30 but less than 61 seats. Proposed § 108.101 (a)(4), however, would expand the applicability to public charter operations as well as private

charter operations using aircraft with more than 30 seats and any type of international operation using an aircraft of less than 61 seats to and from the United States. Such air carriers would not be required to implement all security measures at all times. They would implement portions of their security program only when directed by the Administrator to do so.

Similar to the second level of airport security program requirements, the FAA proposes to expand program requirements for this third category of airports to include establishing procedures for incident response and public advisories. Again, the FAA views these additions as procedural and not unduly burdensome, and believes they would promote a higher level of emergency preparedness.

Specifically, this notice proposes that an airport operator serving air carrier operations specified in proposed § 108.101(a)(4) and existing § 129.25(b)(4) would continue to have in their security program the descriptions of law enforcement support availability and training, the descriptions of a system for maintaining records, and also the identity and means to contact the airport security coordinator. Proposed § 107.103 (c) also would require such airports to include in their security program a description of the following:

1. Airport security coordinator duties and training;
2. A schedule for submitting records;
3. Procedures for handling Security Directives, Information Circulars, and classified information, as appropriate;
4. Procedures for public advisories;
5. Incident management procedures.

The following chart compares security program requirements between airports served by different levels of air carrier operations:

PROPOSED REQUIREMENT	Airport Served By:		
	Scheduled Operations and Public Charter > 60 seats	**Other Schd. Operations and Public/ Private Charter Required to Screen**	**Any Operations not Required to Screen < 61 seats**
Airport Security Coordinator (proposed § 107.5)	x	x	x
Security Compliance Program (proposed § 107.103(a)(2))	x		
Alternate Security Procedures (proposed §107.103(a)(19))	x		
Critical Security Area (proposed §107.201)	x		
Restricted Operations Area (proposed §107.203)	x		
Access Controls (proposed §107.203(b)(1) and § 107.205)	x		
Signs (proposed §107.201(b)(7) and §107.203(b)(7))	x		
Personnel Background Check Procedures (proposed §107.203(b)(2) and §107.207)	x		
Personnel / Vehicle Identification Systems (proposed §107.209)	x		
Escort Procedures (proposed §107.205(d))	x		
Challenge Procedures (proposed §107.209(f))	x		
Training Programs (proposed §107.211)	x		
Law Enforcement (proposed §107.213, §107.215 and §107.217)	x	x	x
Records (proposed §107.219)	x	x	x

PROPOSED REQUIREMENT	Airport Served By:		
	Scheduled Operations and Public Charter > 60 seats	**Other Schd. Operations and Public/ Private Charter Required to Screen**	**Any Operations not Required to Screen < 61 seats**
Contingency Plan (proposed §107.301)	x	x	
Security Directives/Information Circulars (proposed §107.303)	x	x	x
Public Advisories (proposed §107.305)	x	x	x
Incident Management and Notification Procedures (proposed §107.307)	x	x	x

§ 107.105 Approval and amendments

To facilitate the amendment process, this notice proposes that existing §§ 107.5, 107.9, and 107.11 be combined into a single section, proposed § 107.105, and revised to make the process consistent in both parts 107 and 108. Several changes are proposed to the amendment process itself. Proposed § 108.105 prescribes the same approval and amendment procedures.

Throughout this new proposed section, any references to the "Director of Civil Aviation Security" are replaced with "Assistant Administrator." Petition deadlines also have been included for airport operators. Specifically, paragraph (a)(2) proposes that airport operators submit to the Administrator a petition for reconsideration within 30 days after receiving the notice to modify. Paragraphs (d) and (e) of existing § 107.5 have been combined into proposed § 107.105(a)(3) which provide for the Administrator to dispose of any petition within 30 days of receipt. The FAA also specifies, in paragraph (a)(2), that the filing of a petition stays the notice to modify pending a decision by the Administrator. Such timeframes are intended to promote timely and efficient action by both the airport operator and the FAA.

Paragraph (b) of this new section would prescribe procedures for an airport operator to request an amendment to its airport security program now covered under existing § 107.9. Currently § 107.9 states that an airport operator requesting approval of a proposed amendment to its program must submit the request 30 days prior to the effective date of the amendment. The FAA proposes to increase the number days prior to the effective date that the airport must submit its proposed amendment from 30 to 45 days. The proposed rule also notes that the amendment process may take longer than 45 days if the proposed amendment is modified or denied. These languages changes are intended to allow extra time for discussion with the FAA and assist airport operators in planning for program changes.

Existing § 107.9 also states that the FAA will respond to an amendment proposed by the airport operator within 15 days. The proposal extends this time period to provide the FAA with a more realistic period in which to conduct a comprehensive review of the proposed amendment to an airport security program. Under this proposal, the FAA would have 30 days after receipt for approval or denial of the proposed amendment.

In proposed paragraph (b)(4) of this new section, the FAA proposes to modify existing § 107.9(d) to limit the time that an airport operator may petition the Administrator to reconsider the denial to 30 days. Similar to proposed paragraph (a), this requirement is intended to ensure that the airport operator takes prompt action on a petition and permits adequate time to exchange relevant information and support documentation.

Retention of the FAA's existing procedures to amend an airport security program is proposed in paragraphs (c) and (d). Two significant changes, however, are being proposed to the existing procedures of § 107.11: 1) a new requirement for airport operators to submit petitions for reconsideration no later than 15 days before the effective date of the amendment, and 2) a clarification that a petition for reconsideration stays the effective date of the amendment. These changes also are proposed to ensure a timely and efficient exchange of information.

The ASAC recommended that any amendment issued by the FAA to an airport security program include an expiration date. The committee was concerned that the FAA may use the amendment process to circumvent the rulemaking process and suggested that the FAA be required to initiate a formal rulemaking if it wished the provisions of the amendment to continue after the expiration date.

When there is information that cannot be discussed in a public forum, amendment of the security program provides a means to impose and implement a new requirement. The FAA does

not believe it would be in the best interest of the traveling public to require a rulemaking for every amendment to an airport security program, but will establish internal procedures to periodically review amendments to ensure that their inclusion in the security program, rather than part 107, is appropriate.

§ 107.107 Changed conditions affecting security

This proposed section would be new and would include changed conditions that currently require the airport operator to take corrective action under existing § 107.7. It would expand the scope of the requirement to encompass all the elements of the security program. The FAA believes that every element of a security program plays an essential part in the overall integrity of an airport's security system. Therefore, the FAA intends to expand those conditions that must be reported to ensure that any changes that may impact security will be reported to the FAA and addressed as soon as possible.

The proposed rule language reflects the need for the airport operator to report any changes in the physical layout of the airport terminal area that may have an impact on the checkpoint screening operation for which an air carrier is responsible. Similarly, this section proposes to require the airport operator to report any changes in air carrier and foreign air carrier aircraft operations that could lead to a regulatory requirement, such as a change to an air carrier’s level of service, aircraft, or leasehold.

The proposal, like the existing regulation, would establish procedures for the airport operator to follow when a changed condition occurs. Currently, it is necessary for the airport operator to follow routine amendment procedures set forth in § 107.9 (proposed § 107.107) when specific elements of the airport security program change. These procedures would be augmented under

this proposal to require the airport operator to initially notify the FAA within 2 hours, or within an approved timeframe, of the discovery of any changed condition that could affect how an airport complies with regulatory requirements. The availability of electronic communication, overnight delivery services, and local FAA field offices would seemingly provide the means for the airport operator to readily communicate changes to the FAA. While the proposed language provides flexibility in notification time, comments are requested, however, on the feasibility of a 2-hour notification requirement.

This proposed section would require the airport operator during this initial notification to obtain verbal approval of any interim measures to be taken to maintain adequate security. As is currently the case, this proposed section would still allow the FAA to issue an emergency security program amendment under proposed §107.105(d) if an agreement on adequate interim measures cannot be reached. However, new language provides relief in responding to short-term changes.

After this initial notification, paragraphs (c) and (d) propose that the airport operator follow certain procedures to amend its security program to reflect the change. For changed conditions under 60 days' duration, paragraph (c) proposes that the airport operator be relieved from the amendment process required under proposed §107.105 and only be required to provide written notification within 72 hours for FAA approval. Recognizing that many changed conditions affecting security can be readily resolved in less time than it would take to complete the formal amendment process, the FAA intends this change to provide some relief in reporting to the FAA any short-term or temporary changes while ensuring that the FAA retains oversight of temporary or short-term changed conditions to security.

Proposed paragraph (d) of this section would provide procedures for the disposition of changed conditions anticipated to be over 60 days in duration. These procedures are currently used for all instances of a changed condition affecting security.

§ 107.109 Alternative Means of Compliance

This proposed section is new. It would be added to provide relief in certain unique circumstances from the full requirements of an airport security program.

Specifically, it would provide relief for small airports located in communities that are only served by seasonal air carrier or foreign air carrier traffic (such as ski resorts), remotely located, subject to extreme environmental conditions, or have limited facilities and few employees. Often these airports serve aircraft larger than 60 seats for only a portion of the year, or on an infrequent but regular basis (e.g. one operation per day, three operations per week, winter operations only). However, under the definition of proposed § 107.103(a), such airports would be required to have a comprehensive security program. This section would permit the FAA to approve airport operators of such airports to use alternative means to comply with the requirements of the rule.

While air carrier or foreign air carrier operations with aircraft having more than 60 seats necessitate more complex security measures, the FAA recognizes that requiring such airports to implement security measures at the same level of intensity as larger airports would not always be necessary to achieve the required level of security. Currently, the Assistant Administrator can allow for flexibility in applying security measures at such airports, and the FAA proposes to incorporate this process in proposed part 107. To petition for relief from part 107 requirements, larger airport operators would still have to use the exemption process under existing § 11.25, Petitions for rule making or exemptions.

§ 107.111 Exclusive area agreements

The FAA proposes a new section devoted to exclusive area agreements. Existing part 107 includes exclusive area agreements as a provision of § 107.3(b)(3) and (b)(5) and § 107.13, Security of air operations area. As exclusive area agreements are a part of an airport operator's security program and detail part 107 responsibilities assumed by air carriers, the FAA believes that the requirements for exclusive areas should be more closely tied to the airport security program and addressed in a separate section.

Paragraph (a) proposes expanding the existing exclusive area responsibilities for air carriers and foreign air carriers to include individual access points (e.g., doors). The security responsibilities for these points may be assumed by a part 108 air carrier or part 129 foreign air carrier based on an agreement with the airport operator. This section also proposes updating the terminology of the areas in which exclusive area agreements are applied from the air operations area to the proposed critical security areas and restricted operations areas.

In 1992, the FAA initiated a test program to allow several all-cargo carriers to enter into exclusive area agreements with airports by which they assumed the responsibility for control of access to and movement within their leaseholds. The requirements of part 108 do not apply to all-cargo carriers. The test program has been successful and the FAA proposes to allow all-cargo carriers which have voluntarily implemented security programs under part 108 to enter into exclusive area agreements with airport operators.

§ 107.113 Airport tenant security programs

This new section proposes to permit the use of airport tenant security programs that allow airport tenants other than air carriers or foreign air carriers to assume some of an airport operator's security responsibilities, as specified in 49 U.S.C. 44903(c)(2).

While statutory language does not require the FAA to approve airport tenant security programs, the FAA believes the judicious use of such programs would result in better compliance by more directly involving airport tenants in the implementation of security measures. The FAA is concerned, however, that under an airport tenant security agreement, security violations and the associated monetary penalties could be viewed as a justifiable cost of doing business. In order to counter that possibility, the proposal would require the airport tenant security program to specify not only the enforcement steps, but also the point at which the airport tenant security program would be terminated if the tenant continued to violate it.

While similar in concept to the air carrier exclusive area agreement, the airport tenant security program language would differ in an important matter - the tenant would be responsible to the airport operator rather than directly to the FAA. The airport operator would function much as the FAA does by performing compliance and enforcement functions. The tenant security program would have to specify the measures by which the tenant would control access and meet other part 107 requirements on its leasehold. These measures would have to be agreed upon by the FAA, the airport operator, and the airport tenant, and specified in a written agreement within the security program.

Statutory language requires a security program of an airport tenant to include the methods the airport operator will use to monitor and audit the tenant's compliance, the enforcement procedures used in cases of non-compliance, and a provision requiring the tenant to pay financial penalties to the airport operator if the tenant fails to carry out its security responsibilities. This

last provision would require the program to include the dollar amount of fines and other penalty action for each type of violation.

An airport operator complying with all measures for security compliance with a tenant security program, as outlined in its airport security program, may not be found in violation by the FAA for security violations occurring on the tenant's leased area. However, this section should not be misconstrued as diminishing to any degree the requirements reflected in the airport security program or the airport operator's regulatory responsibilities. Paragraph (d) also would specify that the FAA may terminate an airport tenant security program at any time if the tenant fails to provide an acceptable level of security.

The FAA requests comments from airport operators and airport tenants not regulated under part 108 who would be affected by this proposed section. Specifically, any recommendations for procedures or policy that the FAA should issue regarding implementation of this section are welcomed.

Subpart C - Operations

§ 107.201 Security of the critical security area

This proposed new section would provide a more simplified approach to designating areas to be controlled for security purposes. As proposed, there would then only be two types of protected areas, and security measures would be prescribed separately for each. The specific requirements of these measures would be found in subsequent sections of the proposed rule.

Existing part 107 requires the airport operator to designate a portion of the airport where security measures are applied to protect areas used for "landing, taking off, or surface maneuvering of airplanes." This area is called the air operations area (AOA) and existing

§ 107.13 prescribes standards for controlling access and movement of persons and vehicles within it. The specifics of how an airport operator meets these standards are detailed in its airport security program.

The current regulation also requires airports served by larger air carrier aircraft to use stringent access and identification controls within certain portions of the AOA. One of these portions, the secured area, was created with existing §107.14, Access control system. Section 107.14 requires the implementation of complex access control measures in certain portions of the AOA where air carriers operate. The FAA also required airport operators 2.5 years later to implement additional identification display and training procedures to provide even more protection to air carrier aircraft within a portion of the AOA. Designated as the Security Identification Display Area (SIDA), this portion of the AOA overlaps or is identical to the secured area.

The interrelated nature of the AOA, the secured area, and the SIDA has created considerable confusion in the aviation community. The secured area has frequently been misinterpreted to mean all areas of the airport controlled for security purposes. The extent of its application has been regularly disputed, and it is often considered to be independent of the AOA. Likewise, the scope of the AOA has become unclear, and the term is used within the industry and the FAA for other purposes. For example, Advisory Circular 150/5370-10A, Standards for Specifying Construction of Airports, uses the term AOA for safety and construction purposes. Also, the identification requirements of the SIDA are commonly confused with access control requirements of the secured area.

The ASAC expressed dissatisfaction with the terms being used to describe existing security areas and recommended that current terms and requirements be regrouped into two areas only:

the Restricted Operations Area (ROA) and the Secured Operations Area (SOA). As proposed by the ASAC, the SOA would essentially replace the secured area and the SIDA, and the ROA would replace the air operations area.

The FAA believes that the terms "SOA" and "ROA" are too similar and could be inadvertently interchanged, resulting in further confusion and misunderstanding. Instead, to accomplish the same purpose, the FAA proposes the terms "critical security area" as the area with the highest level of security. This area would be approximately that of the current secured area. The term ROA would apply approximately to areas now termed "AOA." The FAA also proposes to require the continuous display of airport-issued or airport-approved identification media in all areas to be secured. This change would apply current SIDA requirements to all critical security areas and restricted operations areas, thus eliminating the need for a separate display area.

A tightly controlled identification system can be used in tandem with access control measures that may not necessarily meet all of the performance standards of proposed § 107.205(a), such as group access, to achieve an acceptable level of security. By requiring identification media to be displayed in both the critical security area and the restricted operations area, identification media would be used as a means to comply with the requirement to control movement to and from such areas. The FAA continues to view identification systems as one of the most effective means to control movement in any portion of a critical security area or restricted operations area.

Proposed § 107.201 would require the airport operator to establish a critical security area and implement certain security measures in this area. The proposed critical security area essentially would replace the secured area that originated with existing § 107.14. Consistent with existing

FAA policy, only the most critical security sensitive portions of an airport would need to be designated as critical security areas. Generally, those portions of the airport are the nonpublic areas where passenger and baggage operations are conducted. Adjacent areas to passenger and baggage operations also may be included in the critical security area if such areas cannot be separated by security measures such as time and distance or a physical barrier. The intent is to more clearly describe the areas of the airport in which security interests are the most critical, and security measures should be applied accordingly.

The following table illustrates the differences in security requirements between the proposed critical security area and the proposed restricted operations area:

Requirements	Critical Security Area	Restricted Operations Area
Complex Access Controls	**x**	
Baseline Access Controls		**x**
Escort Procedures	**x**	**x**
Personnel and Vehicle Identification System	**x**	**x**
Continuous Display of Identification	**x**	**x**
Challenge Program	**x**	**x**
Employment History Verification	**x**	**x**
Criminal Records Check	**x**	
Security Training	**x**	
Security Briefing		**x**
Signs	**x**	**x**

The FAA proposes that airport operators be required to use access controls in the critical security area that meet the current requirements of § 107.14 (proposed § 107.205 (a)). Airport operators and air carriers have invested considerable resources implementing the access control requirements of existing § 107.14, and the FAA believes this investment has resulted in greater protection of the areas that provide access to air carrier aircraft. While operational difficulties have been encountered with the use of these controls, the FAA will continue to support their use and work with airport operators to address operational concerns, such as efficient control of group access (see the discussion below of proposed § 107.205, Access control systems).

The FAA also proposes to continue to require identification in the critical security area, but to further simplify regulatory requirements, training and identification requirements would no longer be linked together as currently prescribed in § 107.25. Instead, this notice proposes to separate requirements for training and for identification systems that the airport operator must implement in critical security areas and restricted operations areas. Proposed § 107.201 would establish the requirement for an identification system that incorporates the standards of proposed § 107.209, including the implementation of a challenge program.

Identification systems are already in use at most airports covered by this section of the proposal, and the FAA contends that such systems are essential. Further, the inclusion of access control and identification requirements also permits the United States to meet its obligations under the Convention on International Civil Aviation to comply with International Civil Aviation Organization (ICAO) Standards. ICAO's Annex 17 to the convention establishes international security standards and recommended practices. Standard 4.4.1 of Annex 17 requires member

states to establish procedures and identification systems to prevent unauthorized access by persons and vehicles to security areas of an airport.

Under this section, individuals with unescorted access to the critical security area would continue to be required to submit to a personnel background check as required under existing § 107.31 and receive training consistent with that currently required in § 107.25. FBI criminal history checks are required for those applying for access to the critical security area if designated "triggers" are raised during an employment history review and verification. The standards for access investigation are contained in proposed § 107.207 .

Proposed § 107.201(b)(6) would require the airport operator to train individuals in a manner prescribed in proposed § 107.211 prior to authorizing such individuals unescorted access to the critical security area. The training requirement outlined in proposed § 107.211 is consistent with the underlying principle that the critical security area is the focus of the airport operator's security measures. Therefore, proposed training requirements would be more involved for the critical security area than for the restricted operations area.

This section also proposes to incorporate signage concepts from FAA Advisory Circular 107-1 (May 19, 1972). This advisory circular recommends that airport operators appropriately post signs warning of the entry restrictions to certain areas at the airport and any penalties associated with unauthorized entry. Proposed paragraph (b)(7) of this section would make this a requirement. Rather than establish specific sign dimension or wording, the proposal sets a broad standard for signs, recognizing the different physical and operational characteristics of individual airports.

The FAA proposes that the airport operator be permitted 2 years to implement the revised sign requirements. This would allow the airport operator time to coordinate sign modifications

with other changes proposed in this section, such as identification systems and training. (See the proposed Implementation Schedule below.)

§ 107.203 Security of the restricted operations area

As discussed in the analysis of the critical security area, the FAA proposes in this new section to require the designation of a restricted operations area and to specify security measures that must be implemented in it.

The restricted operations area concept is based on the current AOA requirements, but the area to be protected would be further explained. Although impossible to fully define for all airports, in general, restricted operations areas would be those areas where air carriers and foreign air carriers subject to parts 108 and 129 take off, land, taxi, park, and otherwise maneuver their aircraft (other than the critical security area), and adjacent areas that cannot be separated by other security measures. This would permit excluding some areas not used by such air carriers and foreign air carriers. It would require including some areas adjacent to runways and taxiways that cannot be separated by secondary controls.

Security measures similar in concept to the those of the critical security area have been proposed for the restricted operations area to strengthen the overall airport security system, but with less complex standards for access control, training, and employment background checks commensurate with the less vulnerable operations within the restricted operations area.

Similar to the differences between the access control requirements of existing §§ 107.13 and 107.14, the means used to control access to and movement in the restricted operations area can differ from the standards to be employed in the proposed critical security area. The FAA proposes that airport operators be required to use access controls in the restricted operations area

that meet the current requirements of § 107.13 (proposed § 107.205 (b)). However, unlike existing § 107.13, this section proposes additional accountability procedures (see the discussion below under proposed § 107.205, Access control systems) .

As in the critical security area, this section proposes that airport operators use an identification system to control movement that meets the standards prescribed in proposed § 107.209.

The expansion of identification requirements is not supported by the ASAC. The committee urged the FAA to limit identification requirements to the secured area (proposed critical security area), leaving the airport operator the discretion to use an identification system in other areas. The FAA acknowledges the need for airport operators to have the latitude to address local circumstances but believes that, if airport identification systems can be bolstered, more pressing operational concerns raised by the implementation of access control systems can be addressed with greater effectiveness. The more stringent identification measures proposed here permit the FAA to propose permitting group access and secondary access media standards under proposed § 107.205.

The FAA proposes to require that the airport operator implement the same escort and challenge procedures used in the proposed critical security area; however, access investigation would differ. This section proposes to require existing employment history verification standards currently used in the AOA. This section also proposes requirements for signs similar to those of the critical security area.

§ 107.205 Access control systems

The FAA proposes in this section to specify the requirements for access control systems that are required in proposed § 107.201 and, in some cases, proposed § 107.203. The performance standards of existing § 107.14 are included in proposed paragraph (a) with modifications, and new procedures are proposed to address operational issues that have come about since the implementation of existing § 107.14.

Specifically, the existing performance standard requiring a system to limit access by time and date has been modified to emphasize that this standard is for contingency purposes only. During a recent review of contingency plans (see the discussion below under proposed § 107.303, Contingency plans), airport operators and air carriers expressed concern about the burden placed on airport operators to meet this performance standard. The ASAC concurred and suggested that the rule clarify that this performance standard be used for contingency purposes only.

Both airport operators and air carriers have urged the FAA to develop technical specifications for access controls. This recommendation also was supported by GAO. The FAA agrees that there is a need for technical standards and is supporting current efforts to develop them, but does not consider the revised regulation as the proper venue to issue technical standards. (See the discussion below entitled “Universal Access System.”)

Existing paragraph (b) would be replaced by access requirements for the restricted operations area. While these requirements are similar to existing § 107.13, the FAA proposes additional accountability procedures. Currently, § 107.13 only requires the airport operator to use procedures to detect and respond to penetration of the AOA and does not specify any other performance or technical standards that such access controls must meet. To ensure better control of access media, proposed accountability procedures would include regular audits of issued

access media, and measures to ensure that access controls are locally controlled and cannot be used to gain access to the restricted operations area of other airports.

Paragraph (c) is proposed to address concerns raised by the ASAC on the issuance of temporary access media to individuals who are not in possession of their original access media. A typical example of this is an airport or air carrier employee who shows up for work without her/his approved access medium and cannot practicably be escorted throughout her/his assigned shift. The existing regulatory language does not address this situation, but such temporary access media generally have been prohibited by local FAA guidance. This paragraph proposes to allow the airport operator to issue a second access medium to an individual as long as access authorization is verified, and other specific standards are met.

Paragraph (d) proposes that the airport operator establish and implement escort procedures for individuals without access authority. Many airport operators already have some type of escort procedure in place based on FAA policy guidance, but such procedures are applied inconsistently. To ensure a more consistent application of these procedures, the FAA believes escorting standards should be incorporated into the rule.

This proposed section also addresses the issue of individual validation and group access. FAA airport inspections that were prompted by the IG audit revealed that, despite best efforts, there are certain instances where individual validation of access authority has become operationally unfeasible. Performance standards require an access control system that validates an individual's access authorization; however, unauthorized group access, commonly known as "piggybacking," often occurs. In such an instance, an individual with assumed authorized access passes through an access point without being subject to any control measures that validate authorization for that individual’s access. As a result, the FAA is reviewing alternative access

measures to accommodate group validation of individual access authorization. The FAA is currently conducting field tests of possible solutions.

To support this effort, the FAA is proposing paragraph (e) to allow airport operators to address the issue of group access. The present performance standards do not allow for group access, but this new language would allow the FAA to work with each airport operator to resolve the issue locally.

Comments regarding the practicality of group access are requested. Any recommendations on methods currently used for access of more than one authorized individual in a vehicle or more than a single individual at an access point would be helpful. For example, local procedures have been developed by some airports that allow for access validation of all persons in a vehicle without requiring each passenger in the vehicle to validate her/his access authorization by individually using the medium (e.g., by "swiping" a magnetic card).

Proposed paragraph (f) would address access control points that lead from non-public areas, other than critical security areas, to the sterile area. Such non-public areas would include air carrier offices and storage areas. In some airports, a sterile area can be accessed via points other than the passenger-screening checkpoint. While current policy partially addresses access to the secured area from the sterile area, very little guidance exists for access to the sterile areas other than the passenger screening requirements of part 108. This rule would clarify that an individual could not be escorted from, for instance, a critical security area, into a sterile area and bypass the screening requirements of part 108.

Paragraph (g) of this section proposes to incorporate the current provisions for alternative access systems. Based on field experience, alternatives would address the use of the passenger-screening checkpoints as an acceptable access control measure used in combination with other

control measures. Further, this paragraph intends to permit alternatives for access controls measures on portions of the ramp where aircraft park or maneuver that lack physical barriers, such as doors or walls, on which to install traditional access controls. The SASP will also provide airport operators more guidance on acceptable alternatives to address unique physical or operational circumstances.

Special Discussion on Universal Access System (UAS)

The implementation of existing § 107.14, Access Control Systems, resulted in many different airport access control systems nationwide. Such variances created access problems for air carrier air crews, whose duties require that they regularly travel to many different airports. Typically,air crews must either obtain separate access media at every airport to which they fly or be escorted through access control points. The aviation industry made several attempts to remedy this situation; however, due primarily to financial constraints, was unable to resolve the problem.

Eventually, pilot groups and air carriers turned to the ASAC for assistance. The ASAC responded by organizing a working group to research, develop, and test standards, and devise an implementation plan for a national access control system that would permit transient air crewmembers to carry a single access control medium which will work at each airline's . An air carrier or airport operator could implement such a system at either a select number of access points or incorporate it into its entire access control system.

In October 1993, Congress appropriated $2 million dollars for development and testing of Universal Access System (UAS) standards. The FAA and the ASAC's UAS Working Group (UASWG) have used these funds to develop preliminary standards and functional requirements, and to field test prototype installations. During this process, the ASAC also expressed interest in

developing standards for all access control systems. The committee decided to use the services of (RTCA, Inc.), another federal advisory committee, to organize this effort, building on research and standards developed by the UAS Working Group. At the request of the industry, the FAA served as a co-chair of this RTCA group, which has since completed its work and compiled its recommendations into RTCA document #D0230. Once UAS standards are finalized, Appendix E of this document will be updated to include specific UAS standards. These tests were conducted in cooperation with volunteer air carriers and airports, including Northwest Airlines andDelta Air Lines; the Detroit Metro Wayne County Airport,and Miami International Airport. Testing .has been completed and a final test report is under review. Next, the preliminary standards will be revised and the UAS working group will address implementation issues.

Since these UAS access points will be held to §107.14, there is no immediate need to modify part 107 or part 108 to accommodate anticipated use of the UAS. Procedural changes which result from a UAS installation will be handled by amendment to the Air Carrier Standard Security Program (ACSSP) or airport security programs (ASP), as appropriate.

§ 107.207. Employment history, verification, and criminal history records checks.

The White House Commission on Aviation Safety and Security recommended, and the Federal Aviation Reauthorization Act of 1996 required, that the FAA adopt rules to provide for expanded background checks and criminal history records checks of persons with responsibilities for screening passengers and property. On March 14, 1997, the FAA issued a Notice of Proposed Rulemaking to respond to these mandates (62 FR 13262, March 19, 1997). The comments received in response to that notice will be considered in developing a final rule. However, while that notice refers to unescorted access to the SIDA, under this proposal the term

SIDA would no longer be used. It is proposed instead that the rule would refer to unescorted access to critical security areas. Under this proposal, existing § 107.31 would be moved to proposed Subpart C, Operations, under new § 107.207.

§ 107.209 Identification systems

Under this proposed new section, an identification system would be required for both the critical security area and the restricted operations area. The FAA would add this section to regulate standards governing the issuance, display, and accountability of identification systems to promote their effectiveness. This proposed section would also comply with ICAO's Annex 17, Standard 4.4.1 that requires member states to establish identification systems to prevent unauthorized access by persons and vehicles to security areas of an airport.

While most airports currently use identification systems of some type to satisfy the movement control requirements of existing § 107.13, there has never been a regulatory requirement to have such a system. Many of the standards and criteria in this proposal, however, have long been included in many airport security programs and , as a result of an 1987 program amendment, national standards for such systems were established. Thus, any system currently in place most likely would require little, if any, alteration to be in compliance with the rule as proposed. Even proposed standards for auditing and vehicle identification not found in the 1987 amendment codify common industry practice.

In addition, the FAA is proposing that the standards would become effective 2 years after a final rule is adopted, providing airport operators with time to make necessary changes so that their systems would meet regulatory requirements.

The ASAC requested that airport operators be afforded 5 years to phase in any identification changes required by the revised rule; however, the committee did not provide any financial or operational data to support this position. As the implementation of proposed identification requirements is dependent on the implementation of other security measures in this proposal, the FAA recognizes that it will take some time to make all the proposed changes. Even so, the FAA sees benefits to bolstering airport identification systems and considers 5 years to be impractical for implementation of the proposed identification requirements. Two years has been proposed based on data collected for the economic analysis for this rulemaking. The FAA requests comments on this schedule, including information regarding operational and cost impacts (see the proposed Implementation Schedule below).

In proposed § 107.209(b), standards are proposed for personnel identification media. Under this proposal, the media must convey accurate information about the individual, bear an expiration date, be readily identifiable for challenge purposes, and indicate the individual's authorization for access and movement. These specifications are similar to those contained in FAA policy and establish broad parameters rather than specific sizes, colors, or actual wording that must appear on the media. The airport security program would state how the individual airport would meet these standards. This would permit considerable flexibility to the airports and accommodate technological advances.

This new section also proposes that an airport operator's identification system include procedures to incorporate identification display requirements of existing §107.25 and to minimize

the number of unaccountable identification media. Accountability requirements are intended to ensure the integrity of the system by specifying an audit at least once a year and media revalidation or reissuance procedures when there is no accountability for a certain percentage of identification media. Procedures are also proposed that would require airport operators to retrieve expired identification media and safeguard unissued identification media stock and supplies. These standards would apply to personnel and vehicle identification systems separately.

The ASAC commented that an audit every 2 years is sufficient and recommended that any requirements for audits not be specified in the revised regulation but included in an airport's security program. While it has been the FAA's policy to require an audit every 2 years, many airport operators have resisted, claiming that the regulation did not require them to do so. The FAA proposes to resolve any misunderstandings about the need to audit identification systems by including the requirement in the regulation.

The FAA views identification systems as one of the most effective means to control movement in any portion of the proposed critical security area or the proposed restricted operations area. As such, the proposal also intends to increase the frequency of the audit to once a year to ensure the integrity of an airport’s identification system. Many airport operators already have automated identification systems that conduct audits on an on-going or daily basis. The proposed annual audit reflects this advance in technology while allowing leeway for less sophisticated identification systems. The inclusion of the phrase "and as necessary" with the 1-year requirement is intended to ensure that an identification system is audited whenever the integrity of a system is in question.

Initially, the FAA considered requiring an airport operator to revalidate its system if 5 percent of identification media were unaccountable. This would codify internal FAA guidance on unaccountable identification media which has been incorporated into most airport security programs. Many airport operators, however, have complained that the 5 percent requirement requires revalidation or reissuance of media too frequently and does not account for the operational reality that employees will lose or misplace identification. The ASAC also expressed similar concerns that this percentage is too low and recommended that the percentage be increased to 10 percent. This recommendation was not supported by any financial or operational data.

Recognizing the serious economic implications associated with revalidation or reissuance of identification media, the FAA has researched accountability percentages and found such percentages to range from 2 percent to 10 percent, depending on whether the identification system is used in a military, civilian, or commercial application, and the layout of the facility. As there appears to be no clear consensus as to the appropriate percentage level for use at airports, the FAA requests comments on what criteria should be the basis for accountability percentages and what these percentages should be. Comments should be supported by financial and operational data and the impact on the integrity of the identification system.

It is anticipated that initial accountability criteria and percentages will have to be tested over an extended period of time and amended as appropriate. To facilitate this process, the FAA proposes that guidance on accountability criteria and percentages be included in the SASP to permit the FAA to be more responsive to operational needs and technological changes. Thus, the revised rule only proposes that the airport operator revalidate its system or reissue badges when a certain accountability percentage identified in the airport security program is reached.

As proposed, revalidation and reissuance percentage would be based on issued identification media. The term issued would apply to any identification medium currently assigned to an individual or vehicle. Returned media should be considered accountable when an individual or vehicle no longer has access and movement authorization.

Additionally, the same standards are proposed for vehicle systems as proposed for the personnel identification system. The FAA is concerned, however, that these standards may not permit the use of existing vehicle identification systems based on specific vehicle markings or paint schemes. If such systems incorporate accountability procedures, airport operators may be allowed to use painting or marking schemes to meet the vehicle identification requirements of this proposed section. Recommendations are requested on standards that will accommodate such vehicle identification but still provide for accountability and integrity of the system.

At ASAC's suggestion, the FAA also proposes in § 107.209(c) to permit the use of the identification program for vehicles used under part 139, if that system also meets the requirements of this proposed section.

Paragraph (d) proposes that airport operators would be required to issue temporary identification media to persons whose duties are expected to be temporary, such as contractors. To minimize the number of accountable and valid identification media, the FAA proposes that such individuals should have their identification media valid only for the time needed to perform their temporary duties.

The FAA further proposes in this section to allow an airport operator to approve the identification media of other entities which meet the standards of this regulation. Inclusion of this practice would codify an acceptable practice used by many airports. The most common example is an air carrier issuing identification media to its employees that in turn are acceptable

to the airport operator for movement and access authority. The FAA also issues identification badges to certain FAA Aviation Safety Inspectors (ASI's) to replace locally issued airport identification media when ASI's are conducting inspections outside their assigned geographical area. Such FAA-issued identification is known as FAA Form 8000-39 and guidance on the acceptance of this identification will be provided in the SASP.

Paragraph (f) proposes to require an airport operator to develop a challenge program. Airport operators currently establish their own challenge procedures to meet the requirements of existing § 107.25(e)(2), but in this paragraph the FAA proposes to expand these requirements in order to ensure standardized challenge procedures between airports, and within the critical security areas and restricted operations areas. The FAA believes consistent challenge procedures will simplify the challenge process for employees, and thereby promote better compliance with identification media display and challenge requirements. The particulars of the challenge program, however, would remain detailed in the approved airport security program. Even though the ASAC did not support standardized challenge procedures, the FAA believes that the lack of standardization has resulted in inconsistent challenge procedures among employees at a given airport, as well as employees who perform their duties at different airports. As a result, the effectiveness of a fundamental element of the airport security program is being undermined.

§ 107.211 Training

This proposed section would remove the training requirements from existing § 107.25 currently titled "Airport identification media" and place them into this new section which would be devoted solely to security training requirements. The change is intended to emphasize the

need for individuals with security responsibilities to be properly trained so that they will be better prepared to fulfill their security duties and responsibilities.

The underlying principle of this proposed section is that individuals who have access to those areas where air carriers conduct passenger enplaning/deplaning operations would have more critical security responsibilities than individuals whose access is limited to peripheral areas of an airport. Accordingly, the FAA proposes a two-tiered training program that would provide security training for individuals with critical security area access authorization and security information to individuals with restricted operations area access authority. Thus, the training would be appropriate for the scope of the individual's access and movement privileges.

Under this section, the FAA proposes that persons with critical security responsibilities should be subject not only to the proposed requirements but also to the training curriculum currently required under existing § 107.25. This enhanced curriculum would promote consistent national implementation of security measures. As proposed, security training would include instruction on the identification system, challenge and escort procedures, restrictions on divulging sensitive security information, falsification of records, and other security responsibilities under proposed § 107.11.

All individuals who have unescorted access to, and movement privileges within, the proposed restricted operations area would be provided with information commensurate with their security responsibilities under this proposal. Security training for those individuals with access to the restricted operations area would be generally the same as that for the proposed critical security area; however, security training for the restricted operations area could be accomplished in a less formal manner and could be provided through a simple videotape presentation, printed material, or verbal presentation.

In addition, this proposed section would direct the airport operator to ensure that persons performing security functions for the airport are briefed on their responsibilities under the proposed rule, the airport security program, and any other pertinent security information.

This proposed section also would specify requirements for maintaining documentation of training and the deadline for implementing a revised training syllabus.

§ 107.213 Law enforcement support

Under this proposal, existing § 107.15 entitled “Law enforcement support” would be renumbered to proposed § 107.213 and revised. Several changes are proposed for the law enforcement support requirements of existing § 107.15. Under existing § 107.15, airport operators must provide law enforcement to support its security program; to support the passenger-screening system required by proposed part 108 and existing part 129; and to respond to an incident at the request of an air carrier or a foreign air carrier.

As stated in the discussion of proposed § 107.3, Definitions, above, the term "law enforcement officers" has been replaced by the term "law enforcement personnel." Existing part 107 uses the term "law enforcement officer" to describe State or local law enforcement and private security personnel, resulting in confusion about the use of private security personnel to support the airport security program and passenger screening functions. This confusion may be the result of the law enforcement community using the term "law enforcement officer" solely to describe qualified Federal, State, or local municipality law enforcement officers. Yet, 49 U.S.C. 44903(c) allows for the use of Federal, State, or local law enforcement officers as well as private security personnel to support airport and air carrier security programs.

To avoid any further misunderstandings, the FAA proposes to use the term "law enforcement personnel" throughout revised part 107 to generically describe both law enforcement officers and private security personnel meeting the requirements of part 107. This would not change the requirements for the type of law enforcement personnel an airport operator can employ.

Existing § 107.15 (a) has been modified to specify the qualifications of law enforcement support required under proposed § 107.103 (a) and (b). However, the most substantial change made to this proposed section would be the distinction between the use of uniformed and "plainclothes" law enforcement personnel.

Currently, § 107.17(a)(2) requires law enforcement support to be identifiable by uniform. Proposed § 107.213 (a) would state that an airport operator need only provide uniformed law enforcement personnel in support of the passenger-screening system required under proposed part 108 and existing part 129. This change was suggested by the ASAC which recommended that airport operators be permitted the leeway to use "plainclothes" law enforcement personnel. The FAA partially concurs with this recommendation and believes that the airport operator, in most cases, is best suited to determine the local need for uniformed and "plainclothes" officers.

This modification would allow law enforcement personnel to operate covertly in situations the airport operator deems appropriate, such as investigating theft in the baggage make-up areas, while requiring a readily identifiable law enforcement presence at the passenger-screening checkpoint. The passenger-screening checkpoint presents a unique situation where individuals subjected to security measures may become uncooperative, and suspect bags and individuals must be successfully segregated in highly congested, often restricted, areas of the airport terminal. The FAA believes that passenger-screening efforts would be better supported by a

prompt response by uniformed law enforcement personnel who are readily identified as having the authority to take charge of the situation.

Paragraph (b) also would be modified to clarify its applicability to the airport security program required under proposed § 107.103(c).

§ 107.215 Law enforcement personnel

Under this proposal, existing § 107.17 entitled "Law enforcement officers" would be renumbered to proposed § 107.215, retitled "Law enforcement personnel," and revised.

The minimum standards for law enforcement support at an airport essentially would be unchanged. As discussed in proposed § 107.213 above, the requirement for law enforcement personnel to be in uniform would be modified. To reflect this proposed change, proposed § 107. 215 (a)(2) would be amended to delete the uniform requirement.

Currently, § 107.17(c) requires that law enforcement officers meet the training standards, if any, prescribed by either the State or local jurisdiction for officers performing comparable functions. Proposed paragraph (c) would update training requirements for State and local law enforcement officers to reflect the fact that all States have law enforcement training programs. This paragraph also would specify that private security personnel used to meet the requirements of part 107 must be trained in a manner acceptable to the Administrator if the State and local jurisdiction does not prescribe training standards for such personnel.

§ 107.217 Supplementing law enforcement personnel

Under this proposal, existing § 107.19 entitled "Use of Federal law enforcement officers," would be renumbered to proposed § 107.217, retitled "Supplementing law enforcement

personnel," and revised. Proposed § 107.217 would give the Administrator greater flexibility in responding to requests to supplement local law enforcement personnel. This revised section still would set forth the same procedures for an airport operator to request Federal assistance in supplementing local law enforcement, but would incorporate statutory language that would provide for supplemental support from any personnel employed by the Federal government.

§ 107.219 Records

Under this proposal, existing § 107.23, entitled "Records," would be renumbered to proposed § 107.219 and revised. Proposed § 107.219 would incorporate new recordkeeping requirements found throughout the proposed rule and would ensure that the FAA has access to such records. This new section would require that law enforcement actions taken in support of passenger- screening activities or the airport security program be recorded, maintained, and submitted to the FAA. Such records would be necessary to measure the effectiveness of the civil aviation security program and to support FAA compliance programs.

Paragraph (a) proposes that the FAA have access to any record required under the proposed rule and would require the submission of records to the FAA pursuant to a schedule approved in the airport's security program. Requiring the airport operator to provide the FAA with a report of law enforcement responses on a regular and predictable basis would prove a more timely and efficient means of disseminating this information to the FAA. The manner in which records are submitted to the FAA, and at what frequency, would be determined for each airport to accommodate local law enforcement reporting and FAA investigation procedures.

A slight modification is proposed for records resulting from law enforcement activity. In proposed paragraph (b)(l) of this section, the word "action" would be changed to "response." A

law enforcement "action" routinely has been confused with "police action" which, within the law enforcement community, suggests some type of detention/arrest or other action related to alleged unlawful activity. In the context of the civil aviation security program, it was intended that a response by a law enforcement entity to any civil aviation security incident needs to be recorded. That response may or may not result from a violation of local law.

Proposed paragraph (b)(2) of this section would extend the period of time during which records must be maintained to a more practical 180 days. Oftentimes, the current 90-day requirement is insufficient for investigation and enforcement purposes. Proposed paragraph (c) would be expanded to require records to reflect more specific information about individuals who are detained or arrested, which would aid the FAA and the FBI in the investigation of such incidents.

The addition of proposed paragraph (d) of this section would require the airport operator to make and maintain for 180 days records of any corrective action taken against persons who fail to comply with proposed falsification and security responsibilities sections (proposed §§ 107.9 and 107.11). A new paragraph (e) is also proposed to require the airport operator to maintain any additional records that may be needed to support the airport security program, and highlight additional recordkeeping requirements found throughout the proposed rule.

Subpart D -- Contingency Measures

§ 107.301 Contingency Plan

Contingency plans are an existing part of airport and air carrier security programs. They contain security measures that can be immediately and flexibly applied to counter threats that arise quickly. To ensure the integrity of the national civil aviation security

system, the security-sensitive details of the contingency plan cannot be included in a public regulation, but proposed new § 108.307 would include in the proposed rule a 1987 security program amendment (amended in 1994) requiring airport operators and air carriers to have and implement a plan.

The application of contingency measures in response to the Persian Gulf War provided valuable lessons on contingency planning and the FAA used this information to make changes to air carrier and airport security programs. Recently, the FAA and the air carriers thoroughly reviewed these plans to incorporate changes and "lessons learned" from response to the elevated threat during the Persian Gulf War. The method for implementation of these was modified to allow for a greater degree of flexibility, and new test procedures also were adopted. The ASAC endorsed the final product of this effort and supported the codification of contingency plan requirements for this proposed revision of part 108.

This proposed new section would require air carriers to implement FAA-issued contingency measures contained in their security programs when directed by the Assistant Administrator for Civil Aviation Security. It also proposes that airport operators and air carriers test these contingency plans to ensure that all parties involved are aware of their responsibilities and that information contained in the plan is current.

§ 107.303 Security Directives and Information Circulars

This proposed section would be new. It would correspond to proposed § 108.305 and would impose the same requirements upon the airport operator to respond as necessary to Security Directives which may apply to airports.

These proposed measures also reflect modification made to the existing Security Directive process in proposed part 108. Existing part 108 provides that the air carrier shall specify, not later than 72 hours after delivery of a Security Directive, the method by which the measures in the Security Directive "have been implemented," unless the Security Directive provides a different time. This appears to assume that, within 72 hours after receipt of the Security Directive, procedures have, in fact, been implemented. However, if the Security Directive does not require implementation within 72 hours, it is not clear from the existing rule when the implementation methods must be provided to the FAA. The proposed rule would make clear that, unless the Security Directive provides otherwise, within 72 hours after receipt of the Security Directive, the airport operator or air carrier would provide to the FAA the implementation methods that are either in effect or will be in effect when the Security Directive is implemented. In response, the FAA would either approve the airport operators proposed alternative measures or notify the airport operator to modify the alternative measures to comply with the requirements of the Security Directive within 48 hours after receiving proposed alternative measures.

In July 1989, the FAA issued a final rule [54 FR 28982, July 10, 1989] that required the use of Security Directives and Information Circulars as the means to disseminate information to air carriers concerning security threats and appropriate measures to be implemented. The FAA uses Information Circulars for the notification of general information regarding threats to civil aviation security, and Security Directives to notify of specific, credible threat information and measures to be taken.

The FAA did not similarly amend part 107 as it was thought at the time that most credible threats were directed at U.S. air carriers, and the threat to domestic airports was relatively low.

The FAA now believes that the concerns of the airport community and the President's Commission on Aviation Security and Terrorism regarding the coordination of security threat information need to be addressed in this revision of part 107.

Airport operators have repeatedly told the FAA that they are not privy to security information in the same manner as air carriers and, as such, they are often at a disadvantage in responding to a higher level of threat. Comments received from the ASAC echoed this concern. The ASAC recommended that airport operators receive Security Directives and Information Circulars; however, the committee stipulated that the FAA should only issue these documents to airport operators on an information basis only, with no requirement to implement specified measures. In its assessment of the aviation security system, the President's Commission on Aviation Security and Terrorism also stressed the need to have better coordination and communication of security information among the FAA, airport operators, and air carriers.

In proposing this requirement, the FAA has not overlooked ASAC's concerns, however; as Security Directive measures directed at airports are anticipated to be site specific and appropriate for the threat level, the FAA views the benefit of the proposed requirements as a necessary precaution that will not unduly burden airport operators. Further, the FAA in the past has issued emergency amendments to airport security programs to respond to an increased threat. Such emergency measures often may be more efficiently handled by use of Security Directives.

This section also proposes to permit the airport security coordinator to apply for a security clearance through the FAA in order to receive classified information related to national security. Such clearances for airport security officials were recommended by the Federal Bureau of Investigation in a 1992 report, and more recently, by the GAO in the aforementioned audit of FAA’s compliance with the Aviation Security Improvement Act of 1990. The FAA carefully

considered the implications of granting such clearances, particularly the risk of unauthorized release of sensitive information, and subsequently endorsed the issuance of security clearances, on a voluntary basis, to select airport personnel at 74 of the largest and busiest U.S. airports. As of May 1995, 101 clearances had been granted to airport security personnel. The results of this voluntary program have been positive and the FAA believes the dissemination and coordination of security sensitive information among airport security personnel has been enhanced. As such, the FAA proposes to formalize this program in part 107 and permit airport security at all airports regulated under part 107 to apply for a security clearance.

§ 107.305 Public advisories

This proposed new section would be added to incorporate new statutory language and the 1986 airport security program amendment.

In August 1986, the FAA amended airport security programs to require airport operators to notify the public of ineffective security measures at foreign airports. This amendment was issued by the Administrator under the provisions of § 107.11(f) in response to Public Law 99-83; 99 Stat. 222-227, Title V - International Terrorism and Foreign Airport Security, Section 552 (a), Travel Advisory and Suspension of Foreign Assistance. This legislation requires airport operators to immediately post and prominently display the identity of any foreign airport that the Secretary of Transportation determines is failing to maintain and administer effective security measures. The provisions for public notification established in Public Law 99-83 have been included in 49 U.S.C. 44907.

Airport representatives on the ASAC commented that this public notification requirement was ineffective, noting that such postings are typically ignored by the traveling public. They

suggested that only air carriers be required to notify passengers of such airports. Congress has determined, however, that such postings are important to alert the traveling public. The FAA encourages comments and recommendations on how such postings of notifications could be more effectively displayed.

§ 107.307 Incident Management

This new section would be added to require the airport operator to establish procedures to evaluate and respond to threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations. Existing part 107 lacks a requirement for airport operators to respond to threats of such criminal activity. Instead, part 139, Certification and Operations: Land Airports Serving Certain Air Carriers, requires airport operators to be prepared to respond to an actual incident of sabotage, hijack, and other emergencies by developing and testing an airport emergency plan under § 139.325. These emergency procedures are typically incorporated in the airport security program verbatim.

Proposed paragraph (b) would specifically provide that evaluation of a threat would be under the security program. However, any event covered by the part 139 airport emergency plan, such as an actual hijacking, would be handled as specified in the airport emergency plan.

The procedures to evaluate threats may include sensitive security information and, as such, should remain in the airport security program to limit its distribution. The FAA believes that emergency response procedures to such incidents, however, should remain in the part 139 airport emergency plan. An expedited response to emergency situations is critical, and response procedures to any emergency should be limited to one document to minimize delays and confusion.

To promote coordination between parts 107 and 139, the FAA is also proposing to amend § 139.325 to ensure that emergency response procedures to hijack and sabotage incidents contained in the airport emergency plan are consistent with the approved airport security program. Proposed § 107.307(d) would support this coordination by requiring the airport operator to review annually threat and incident response procedures. Such a review is intended simply to ensure threat response procedures and contacts are still accurate and should not be interpreted as a requirement for a full-scale exercise. The FAA anticipates that such a review could readily be incorporated into the annual review of the airport's emergency plan required under § 139.325(c)(4).

In the event that an airport required to have an airport security program under part 107 is not required to have an airport emergency plan under part 139, paragraph (c) proposes to require such facilities to develop emergency response procedures in addition to threat evaluation procedures. This proposed section is intended to ensure such airport operators are prepared to respond to actual incidents of criminal activity and is not intended to require minimum standards for aircraft rescue and firefighting or emergency equipment.

Implementation Schedule

The FAA will include in the final rule an implementation schedule for the transition from the existing requirements to those adopted in the final rule. The revisions to part 107 have been extensive, and the FAA recognizes that airport operators will have to make extensive changes to security measures and airport security programs. The FAA proposes to make new part 107 effective 120 days after the publication of the final rule, unless otherwise noted in the rule. Several sections of the proposed rule, including identification, signs and training requirements

would permit extra time to phase out old security measures and references and introduce new ones. It is anticipated that this transition schedule will be based on airport size and possibly limited to certain requirements that necessitate a longer time period to implement. The FAA is requesting comments on this proposed schedule and recommendations on a feasible implementation schedule and methodologies to facilitate a smooth transition.

Harmonization with International Civil Aviation Organization and Joint Aviation Requirements

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is the FAA's policy to comply with International Civil Aviation Organization (ICAO) Standards and Recommended Practices (SARP) to the maximum extent practicable. As discussed above in the analysis of §§ 107.201, 107.209, and 107.221, the FAA has determined that, where applicable, it has complied with ICAO SARPs in developing this proposal.

ICAO has required strengthened and intensified security programs in response to terrorist attacks. Due to the increased severity of criminal acts against civil aviation, the ICAO Council convened on an accelerated schedule and, on December 19, 1985, adopted Amendment 6 to Annex 17 to the Convention on International Civil Aviation, entitled "Standards and Recommended Practices - Security - Safeguarding International Civil Aviation against Acts of Unlawful Interference." Eleven new specifications were introduced into the Annex and nineteen specifications were adopted as standards. Domestic airport security programs were amended accordingly. In September 1989, the ICAO Council adopted Amendment 7 to Annex 17 which allows it to implement standards and recommended practices at an accelerated pace. In December 1992, the ICAO Council adopted Amendment 8 to Annex 17 which introduced new

provisions for the following: screening checked baggage and controlling cargo, variations to procedures relating to security programs, pre-flight checks of international aircraft, and measures for incorporating security into airport designs.

The Joint Aviation Authorities, an associated body of the European Civil Aviation Conference, develop Joint Aviation Requirements (JAR) in aircraft design, manufacture, maintenance, and operations for adoption by participating member civil aviation. The JAR do not address aviation security.

Paperwork Reduction Act

Proposed §§ 107.5, 107.101, 107.103, 107.105, 107.107, 107.111, 107.113, 107.210, 107.203, 107.207, 107.209, 107.211, 107.215, 107.217 and 107.219 contain information collection requirements. As required by the Paperwork Reduction Act of 1995 (44 U.S.C. 3507 (d)), the FAA has submitted a copy of these proposed sections to the Office of Management and Budget (OMB) for its review.

The information to be collected is needed to allow the FAA to comply with Congressional reporting requirements and to verify compliance with statutory requirements under 49 U.S.C. Subtitle VII to protect persons and property in air transportation against acts of criminal violence.

The collection of information required under this proposal has been in effect for several years, and reporting and recordkeeping requirements have remained generally consistent. While many of the proposed part 107 program amendment and law enforcement record requirements remain virtually unchanged, some additional information collections would be required. For all of the reporting elements in the collections of information contained in this proposal, the annual reporting burden is estimated to be 15,630 hours. For all of the recordkeeping elements in the

collections of information contained in this proposal, total initial annual recordkeeping is estimated to be 753,658 hours and annual recordkeeping burden is estimated to be 388,735 hours.

It is estimated that this proposal will affect 460 part 107 regulated airports annually.

Organizations and individuals desiring to submit comments on the information collection requirement should direct them to the Office of Information and Regulatory Affairs, OMB, Room 1235, New Executive Office Building, Washington, DC 20503; Attention: Desk Officer for Federal Aviation Administration. These comments should reflect whether the proposed collection is necessary; whether the agency's estimate of the burden is accurate; how the quality, utility, and clarity of the information to be collected can be enhanced; and how the burden of the collection can be minimized. A copy of the comments also should be submitted to the FAA Rules Docket.

Economic Summary

The FAA has determined that this proposed rule is not a "significant rulemaking action," as defined by Executive Order 12866 (Regulatory Planning and Review). The anticipated costs and benefits associated with this proposed rule are summarized below. (A detailed discussion of costs and benefits is contained in the full evaluation in the docket for this proposed rule.)

The FAA is responsible for promulgating regulations to provide a safe and secure civil air transportation system. Consistent with its statutory responsibilities, the FAA has adopted Federal

Aviation Regulations (FAR's) dealing with aviation security. These rules include FAR part 107 covering airport security and FAR parts 108, 109, and 129 regulating the security practices and procedures of affected air carriers. These regulations provide specific measures and guidelines to prevent air piracy and other criminal acts. At the time that these rules were promulgated, the primary focus of civil aviation security was the prevention of individual acts of air piracy.

Over the last decade, terrorist and criminal actions against civil aviation have resulted in the continued tragic loss of life and property. This has resulted in the FAA promulgating several emergency rulemaking actions. The FAA has also combatted these terrorist and criminal incidents by imposing specific requirements on airports by amending their individual security programs.

The proposed regulation is an attempt to comprehensively updated airport security regulations. Such a comprehensive review is necessary to address changes to the structure of civil aviation security as well as to analyze the effect of emergency rulemakings on the entire security program. Thus, the FAA is proposing to amend the existing airport security rules to incorporate in the rules certain requirements that had been part of the airports' security programs. (In a parallel rulemaking effort, the FAA is also proposing to amend the existing air carrier security rules, which are contained in part 108.)

The FAA is proposing to revise the current §§ 107.1 through 107.31 and add new sections, some of which address the security responsibilities of individuals. Historically, part 107

has been amended in increments with each amendment added to the regulation in near chronological order. The FAA proposes to reorganize the regulation based on subparts organized by subject matter. Arranging the regulation by subparts allows the FAA to keep operationally similar sections together. This proposed rule groups the sections into four subparts - Subpart A - General (§§ 107.1 to 107.11), Subpart B - Airport security program (§§ 107.101 to 107.113), Subpart C - Operations (§§ 107.201 to 107.219), and Subpart D - Contingency Measures (§§ 107.301 to 107.307).

Currently, there are 460 airports in the U.S. aviation system that have an Airport Security Program (ASP) approved by the FAA; the contents of this program, its approval, and the amendment process are key components of part 107. All airport security programs cover many of the same requirements and concerns. However, due to the different physical layouts and security requirements of each airport, each airport's security program will have some unique features. Accordingly, it is important to note that there is not a single airport security program, but, instead, many programs that have many common elements.

Many of the proposed changes to part 107 simply change definitions or make minor word changes. These changes would not result in any incremental costs and will not be covered in this summary. Nine proposed sections would increase costs, and three proposed sections would result in cost savings. In this analysis, the FAA estimated costs for a 10-year period, from 1996 through

2005. As required by OMB, the present value of this cost stream was calculated using a discount factor of 7 percent. All costs in this analysis are in 1994 dollars.

Proposed § 107.5, entitled "Airport Security Coordinator" (formerly § 107.29), would increase the responsibilities of the Airport Security Coordinator (ASC). Under this proposed rule, the ASC, or in certain cases, the airport operators or their designees, must review materials and security functions for effectiveness and compliance and take corrective action immediately for each instance of non-compliance with this part and immediately notify the FAA of the instances and any corrective measures taken. The ASC must also be trained in accordance with the FAA-approved security program every two years. The estimated cost resulting from these changes total $7.5 million, discounted.

Proposed § 107.11, entitled "Security Responsibilities of Persons" would prohibit persons from tampering, compromising, or modifying any security systems, or carrying a deadly or dangerous weapon, explosive, incendiary, or destructive substances into sterile areas, critical security areas, or restricted operations areas. Proposed § 107.103 would have the FAA require the airport operator to include in its security program procedures to ensure that persons with unescorted access to critical security areas and restricted operations areas comply with the requirements of proposed § 107.11; the cost of this requirements is assigned to proposed § 107.11 as this section is the basis for the compliance program. The cost to implement such a compliance program would include initial compliance program and annual administration of this

program. However, part of the compliance program is the challenge procedure which is covered in proposed § 107.209(f). Thus, the net total compliance costs of $2.7 million, discounted, do not include the costs of setting up and administering a challenge program.

Proposed § 107.103, entitled "Content" (amending the current § 107.3) would expand the requirements for the Airport Security Programs (ASP's) to include descriptions of incidence response and notification procedures, controlled notification signs, and the increased responsibilities of the Airport Security Coordinators. The estimated administrative costs would be approximately $49,200, discounted.

Proposed § 107.107, entitled "Changed conditions affecting security" (amending the current § 107.7) would involve notification costs. All airports are required to alert the FAA to certain changes in airport security. This proposal would increase the number of airport security changes that the FAA needs to be aware of; require each airport operator to notify the FAA within two hours of discovery of these changes and explain the interim measures being taken to deal with them; and relieve airports of having to modify their ASP for a changed security condition under 60 days. This proposed revision would save an estimated $5.1 million, discounted.

Proposed § 107.201, entitled "Security of the critical security area" (amending the current § 107.14) would replace the secured area portion which is subject to the current § 107.14. Only the most critical security sensitive portions of the airport would need to be designated as critical

security areas, such as those areas where passenger and baggage operations are conducted and adjacent areas that are not separated by security controls or physical barriers. The intent is to better define the areas of the airport in which the security interest is the most critical and where security measures should be the most complex. This would entail a number of additional costs including rebadging and training all employees with access to the proposed critical security area, requiring those airports without a personnel or vehicle identification system to establish one, and changing warning notices and signs for this area. This proposed revision would cost an estimated $129.7 million, discounted.

The proposed § 107.203, entitled "Security of the restricted operations area" (amending the current § 107.13), would establish "restricted operations areas." In this area, which would be similar on the current AOA, the means used to control access and movement would not need to be held to the same standards as the means proposed to control access and movement in the critical security area. However, the proposed regulation on restricted operations areas would still entail a number of additional costs including rebadging and providing information to all employees with access to the restricted operations area and changing warning notices and signs for this area. This proposed revision would cost an estimated $12.7 million, discounted.

Proposed § 107.205, entitled "Access control systems" (amending the current § 107.14), would embellish the existing performance standards for access controls by allowing the issuance of a second access medium to individuals. The secondary access media program would give

airport operators an option in addition to using either existing airport escort programs or denying employees access without their original cards, both of which can be very costly. An airport operator opting to use a secondary access media would incur additional costs, including development costs, annual computer time, card manufacturing costs, and card storage costs. A few airports currently escort all employees who do not have their access cards. Most others deny entry to employees without access cards. They are either sent home to retrieve the card or not allowed to work for the day, so that employee's supervisor would need to reassign employees and/or obtain employees from labor pools which exist to insure against employee "no shows". In addition, this proposed section would require airports to ensure that all doors leading from non public areas, other than the critical security area, to the sterile area meet the access control requirements of this proposed section. The total net cost savings would be $4.7 million, discounted.

Proposed § 107.209, entitled "Identification systems" (amending the current § 107.25), would require airports to implement an ID system if they don't have one, and require ID systems to meet certain standards. Such standards would require airports to audit their identification (ID) systems once a year and revalidate their ID systems when a percentage, specified in each airport's ASP, of the currently issued identification media become unaccountable for both personnel and vehicle systems. Airports that do not have personnel or vehicle identification systems would have to install a system and incur administrative costs. In addition, it would

require airport operators to have temporary personnel and vehicle IDs for people without unescorted access authority. In addition, this proposed section would require airport operators to implement a challenge program in the "critical security" and "restricted operations" areas. The purpose of the challenge program is to improve each airport operator's ability to limit unauthorized incursions in the secured area. The proposed rule would require all airports to codify their present challenge programs; airports without such a program would also incur administrative costs. The total costs of this proposed section would be $7.5 million, discounted.

Proposed § 107.215, entitled "Law enforcement personnel" (amending the current § 107.17), would allow for the use of plainclothes officers in support of the airport security program. This is a voluntary program, but the use of plainclothes officers could result in savings. The airport operator could better utilize officers and realize savings in labor costs. The analysis assumes that 5.5 percent of airports would use this option, yielding cost savings of $19.5 million, discounted.

Proposed § 107.219, entitled "Records" (amending the current § 107.23), would require that records be maintained pursuant to a schedule in the ASP and increase the time an airport must maintain records from 90 days to 180 days. Airports would still be required to report all deadly weapon activity, arrests, and threats against civil aviation, but the proposed section would also require the airport operator to maintain records of corrective actions imposed on persons in

support of the security compliance program. The additional recordkeeping and maintenance costs would total $9.4 million, discounted.

The proposed § 107.303, entitled "Security Directives and Information Circulars" would develop standardized procedures that airport operators must follow upon receiving such documents issued by FAA. The administrative time cost required to process and respond to these documents is estimated at a discounted $78,100.

The proposed § 107.307, entitled "Incident management," would require that airports incorporate certain procedures into their ASP's for responding to threats of sabotage, aircraft piracy, and other unlawful acts against civil aviation. This section would also require that airport operation to coordinate these procedures with emergency response procedures required in FAR part 139; the costs of incorporating these threat response procedures into part 107 and the review that would be necessary are estimated to be approximately $1.3 million, discounted.

The 10-year cost of this proposed rule would be $174.5 million (present value, $142.1 million).

The FAA requests comments on the most cost-effective ways to implement these proposals. Many of these proposals are performance standards and do not provide many detailed requirements as to how they could or would be implemented. Thus, the regulated parties may have several options as to how to comply. The FAA, in preparing this analysis, chose what it considered to be a reasonable approach in analyzing and costing out each proposed section, and

recognizes that there may be more efficient ways to implement each section. The FAA requests that comments be as detailed as possible and cite or include supporting documentation.

The FAA points out that, in estimating the costs of the rule, the projected costs may well be in excess of the actual costs of complying with a final rule. Some of the projected costs are significant in terms of the total projected costs of the rule. For example, the designation of "critical secured areas" has total projected costs that could be as high as $129.7 million, compared with total projected costs of $142.1 million, discounted, over 10 years. In terms of implementation, the FAA expects that airport operators would find ways of meeting the objectives of the rule in ways that may significantly reduce costs.

FAR Part 107 contributes to a secure civil air transportation system by providing specific regulations to prevent criminal acts or air piracy. The benefits of the proposed part 107 rules would be a strengthening of airport security. The current airport security systems, in which security is maintained through an intricate set of interlocking requirements, are effective and have prevented terrorist and criminal acts. The proposed changes would simply add to this effectiveness. In a parallel rulemaking effort, the FAA is also proposing to amend the existing air carrier security rules, which are contained in part 108.

The high degree of dependence between parts 107 and 108 and among the proposed amendments does not permit the separation of the benefits of these proposed amendments from the previous rules. It would be extremely difficult to determine to what extent an averted

terrorist incident could be credited to either airport operator security or to air carrier security. Accordingly, the benefits from the proposed rules for parts 107 (airport operators) and 108 (air carriers) have been combined in this benefit-cost analysis.

The benefits of this rulemaking would be the prevention of specific criminal and terrorist incidents, primarily explosions, hijackings, and sabotage. The FAA examined the number of criminal and terrorist incidents from 1985 to 1994 to compute the overall benefits. In order to provide the public and government officials with a benchmark comparison of the expected safety benefits of rulemaking actions over an extended period of time with estimated costs in dollars, the FAA currently uses a value of $2.7 million and $518,000 to statistically represent a human fatality and a major injury avoided, respectively.

The FAA has calculated benefits based on the types of criminal and terrorist incidents that parts 107 and 108 are designed to combat. A Poisson probability distribution was used to assist in estimating the potential benefits of these proposed rules. The Poisson distribution is particularly useful in describing discrete random variables having a low probability of occurrence. Applying this distribution to the actual number of historical incidents results in projected probabilistic estimates of potential future incidents.

The FAA developed the Poisson probability distribution model based on the historical record while assuming that the past level of threat carries into the future. This model was used to estimate the potential number of future criminal and terrorist incidents that may occur in the

absence of aviation security rulemaking actions. What resulted were probability estimations of experiencing such incidents on board U.S. air carriers over the next 10 years. Given the uncertainties of predicting future criminal and terrorist incidents, the FAA is taking a conservative approach and using the historical record of incidents as representative of the true mean of occurrences for incidents, which sums to $1.871 billion (present value, $1.334 billion).

The agency recognizes that potential benefits could change as the result of the changing dynamics of aviation security. While the benefits estimate is valid based on those incidents cited in the historical record, this baseline could change upon the assessment of an increased credible security threat(s). If such information warrants some form of regulatory initiatives, then the historical baseline would be augmented to include those threats. Subsequently, the pool of potential safety benefits could increase and be applied to any future rulemaking actions related to such threats.

Since 1987, the FAA has initiated rulemaking and promulgated five security-related rules[7] that have amended both parts 107 (airport operators) and 108 (air carriers). These rules also added to the effectiveness of both parts in that they were designed to address certain aspects of the total security system to help prevent additional criminal and terrorist activities. These

[7] The five rules are:

- Access to Secured Areas at Airports (1988)
- Security Directives (1989)
- Explosives Detection Systems (1989)
- X-Ray Systems (1990)
- Employment Standards (1990)

rules comprise a portion of the costs of combating the criminal and terrorist incidents that the existing parts 107 and 108 are trying to prevent. Accordingly, these costs can be compared with the benefits of preventing such incidents. To put the proposed changes to parts 107 and 108 into context, the costs of these past rulemakings will be added to the costs of the proposed changes to parts 107 and 108; the benefits will also be contrasted against the costs of all these rulemakings.

In reviewing the five security-related rules, the costs were updated from their respective base-year dollars to 1994 dollars using the implicit price deflator for Gross Domestic Product. The present value of the costs and benefits was recalculated using the current discount rate of 7 percent. The FAA has developed new data that has improved components of past analyses. The estimated updated discounted costs total $498 million.

The FAA has developed three cost-benefit comparisons. Comparing benefits of $1.871 billion, which are based on the historical record of incidents, to the combined estimated costs of the proposed amendments to parts 107 and 108, $217.4 million, suggests that expected benefits exceed estimated costs.

Using the Poisson distribution, the FAA estimated the probability of occurrence of potential benefits. From this information, the agency has been able to determine the probability of obtaining occurrences where potential benefits would exceed costs. Each of the criminal and terrorist incidents, explosions, hijackings, and sabotage, has a range of expected occurrences (based on the current assumed level of threat) with an associated probability for each discrete

number of events. The FAA calculated the probability and associated benefits of each possible combination of occurrences. The results of this analysis indicates that the probability exceeds 95% that obtaining combinations of occurrences where the benefits of avoiding any of these combinations of occurrence will exceed the estimated costs of these proposed rules.

When the estimated cost of these two proposed rules are added to the cost of the five security rules ($727 million, undiscounted) already issued, the combined cost is $944 million, undiscounted. The probability of obtaining a combination of occurrences yielding benefits equal to or greater than $944 million is over 68%. The FAA, therefore, has determined that the benefits of these two proposed rules exceed their costs, even when the costs of these two rules are added to the cost of the previously issued rules.

International Trade Impact Statement

In accordance with the Office of Management and Budget memorandum dated March 1983, federal agencies engaged in rulemaking activities are required to assess the effects of regulatory changes on international trade. This proposed rule would affect all airport owners that have an FAA-approved security program in accord with part 107. Unlike domestic air carriers that compete with foreign air carriers, domestic airports are not in competition with foreign airports. For this reason, a trade impact assessment would not be applicable.

Initial Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980 (RFA) was enacted by Congress to ensure that small entities are not unnecessarily burdened by government regulations. The RFA requires agencies to review rules that may have a "significant economic impact on a substantial number of small entities."

The FAA's criterion for a "substantial number" is a number that is not less than 11 and that is more than one third of the small entities subject to the rule. The FAA's small entity size standards criterion define a small airport as one owned by a county, city, town or other jurisdiction having a population of 49,999 or less. If two or more towns, cities, or counties operate an airport jointly, the population size of each are totaled to determine whether that airport is a small entity. The threshold annualized cost levels in December 1983 dollars is $5,400 for airports; adjusting to 1994 values, this threshold cost becomes is $7,800.

The FAA examined all primary airports[8] to determine the number of airports classified as small entities. After reviewing population data, the FAA determined that 108 of the primary non-military airports are owned by jurisdictions with populations less than 50,000.

Some airports are already in compliance with portions of the proposed rule and the total costs estimated in the regulatory evaluation were adjusted accordingly. However, this regulatory

[8] A primary airport is one which enplanes 10,000 or more passengers annually (as per 49 U.S.C. 47102 (11)).

flexibility determination, in looking for the maximum cost that could be incurred by a small entity airport, assumed that the typical airport was not in compliance. Annually, the proposed part 107 would cost the average Type A (<2) airport no more than $28,299, save the typical Type B airport $3,327, and cost the typical Type C airport no more than $ $2,869.

The cost of the proposed part 107 to Types B and C are less than the threshold figure of $7,800, but the costs of Type A (<2) airports exceed this threshold. As noted above, there are 21 Type A (<2) airports in the 108 airports that qualify as small entities. At 19% of the number of small entities, this is less than the definition of a "substantial number". Therefore, the FAA finds that this proposed rule would not have a significant impact on a substantial number of small entities.

Unfunded Mandates Reform Act

Title II of the Unfunded Mandates Reform Act of 1995 (the Act), enacted as Pub. L. 104-4 on March 22, 1995, requires each Federal agency, to the extent permitted by law, to prepare a written assessment of the effects of any Federal mandate in a proposed or final agency rule that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. Section 204(a) of the Act, 2 U.S.C. 1534(a), requires the Federal agency to develop an effective process to permit timely input by elected officers (or their designees) of State, local, and tribal governments on a proposed "significant intergovernmental mandate." A "significant intergovernmental mandate" under the Act is any provision in a Federal agency regulation that will impose an enforceable duty upon State, local, and tribal governments, in the aggregate, of $100 million (adjusted annually for inflation) in any one year. Section 203 of the Act, 2 U.S.C. 1533, which supplements section 204(a), provides that before establishing any regulatory requirements that might significantly or uniquely affect small governments, the agency shall have developed a plan that, among other things, provides for notice to potentially affected small governments, if any, and for a meaningful and timely opportunity to provide input in the development of regulatory proposals. This proposed rule does not contain any Federal intergovernmental mandates or private sector mandates.

Federalism Implications

The regulations proposed herein will not have substantial direct effects on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. Therefore, in accordance with Executive Order 12612, it is determined that this proposed regulation will not have sufficient federalism implications to warrant the preparation of a Federalism Assessment.

Conclusion

For the reasons discussed in the preamble, and based on the findings in the Initial Regulatory Flexibility Determination and the International Trade Impact Analysis, the FAA has determined that this proposed regulation is significant under Executive Order 12866. In addition, it is certified that this proposal, if adopted, will not have a significant economic impact, positive or negative, on a substantial number of small entities under the criteria of the Regulatory Flexibility Act. This proposal is considered significant under DOT Regulatory Policies and Procedures (44 FR 11034; February 26, 1979).

List of Subjects

14 CFR part 107

Airports, Arms and munitions, Law enforcement officers, Reporting and recordkeeping requirements, Security measures.

14 CFR part 139

Air carriers, Airports, Aviation safety

THE PROPOSED AMENDMENT

In consideration of the foregoing, the Federal Aviation Administration proposes to amend parts 107 and 139 of 14 CFR as follows:

1. Part 107 is revised to read as follows:

Part 107 - Airport Security

Sec.

Subpart C - Operations.

Subpart D - Contingency measures.

Authority: 49 U.S.C. 106(g), 5103, 40113, 40119, 44701-44702, 44706, 44901-44905, 44907, 44913-44914, 44932, 44935-44936, 46105.

Part 107 - Airport Security

Subpart A - General

§ 107.1 Applicability.

(a) This part describes aviation security rules governing:

(1) The operation of each airport regularly serving an air carrier required to have a security program under part 108 of this chapter.

(2) The operation of each airport regularly serving a foreign air carrier required to have a security program under § 129.25 of this chapter.

(3) Each person who is in, or entering, a critical security area, restricted operations area, or sterile area described in this part and part 108 of this chapter.

(4) Each person who files an application or makes entries into any record or report that is kept, made, or used to show compliance under this part, or to exercise any privileges under this part.

(b) Except as provided in § 107.105 of this part, the authority of the Administrator under this part is also exercised by the Assistant Administrator for Civil Aviation Security and the Deputy Assistant Administrator for Civil Aviation Security, and any individual formally designated to act in their capacity. The authority of the Assistant Administrator, including matters under § 107.105 of this part, may be further delegated.

§ 107.3 Definitions.

Terms defined in part 108 of this chapter apply to this part. For purposes of this part, part 108 of this chapter, and security programs under these parts, the following definitions also apply:

"Airport operator" means a person who operates an airport serving an air carrier or a foreign air carrier required to have a security program under part 108 or § 129.25 of this chapter.

"Airport security program" means an airport operator's security program required under § 107.101 of this part and approved by the Administrator.

"Airport tenant" means any person, other than an air carrier or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter, that has an agreement with the airport operator to conduct business on airport property.

"Airport tenant security program" means the agreement between the airport operator and an airport tenant that specifies the measures by which the tenant will perform security functions under § 107.113 of this part.

“Assistant Administrator” means the FAA Assistant Administrator for Civil Aviation Security as described in 49 U.S.C. 44932.

"Critical security area" means a portion of an airport specified in the airport security program in which security measures specified in this part are carried out. In general, this area is where air carriers and foreign air carriers enplane and deplane passengers, and sort and load baggage, and any adjacent areas that are not separated by security controls or physical barriers.

“Escort” means to accompany or supervise an individual who does not have unescorted access authority to a critical security area or a restricted operations area, in a manner sufficient to take action should the individual engage in activities other than those for which the escorted access is granted.

"Exclusive area" means any portion of a critical security area or restricted operations area, including individual access points, for which an air carrier or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter has assumed responsibility under § 107.111 of this part.

"Exclusive area agreement" means an agreement between the airport operator and an individual air carrier or foreign air carrier that has a security program under part 108 or § 129.25

of this chapter that permits such an air carrier or foreign air carrier to assume responsibility for specified security measures in accordance with § 107.111 of this part.

"Restricted operations area" means a portion of an airport specified in the airport security program in which security measures specified in this part are carried out. In general, this area is where air carrier and foreign air carrier aircraft take off, land, taxi, park, and otherwise maneuver (other than critical security areas), and any adjacent areas that are not separated by security controls or physical barriers.

"Unescorted access authority" means the authority granted to individuals by an airport operator, air carrier, foreign air carrier, or airport tenant authorized under this part, or parts 108 or 129 of this chapter, to gain access to, and be without an escort in, critical security areas and restricted operations areas.

§ 107.5 Airport security coordinator.

(a) Each airport operator shall designate an Airport Security Coordinator (ASC), and any alternate ASC as necessary, in the airport security program to serve as the airport operator's primary and immediate contact for security-related activities and communications with the FAA. Any individual designated as an ASC may perform other work duties in addition to those described in paragraph (b) of this section.

(b) The ASC, or alternate ASC, shall -

(1) Serve as the airport operator's primary and immediate contact for security-related activities and communications with the FAA;

(2) Be available to the FAA on a 24-hour basis;

(3) Review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with this part, including the airport security program, airport tenant activities, and applicable security directives;

(4) Immediately initiate corrective action for any instance of non-compliance with this part, the airport security program, and applicable security directives;

(5) Review and control the results of access investigations required under § 107.207 of this part;

(6) Serve as the contact to receive notification from individuals applying for unescorted access of their intent to seek correction of their criminal history record with the FBI; and

(7) Perform any other duties deemed necessary by the Administrator as set forth in the airport security program or in a Security Directive.

(c) Effective [insert 180 days after publication of the final rule in the Federal Register], each airport operator shall ensure and document that the individual designated as the ASC, and each designated alternate ASC, has been trained within the preceding 24 calendar months to carry out the responsibilities described in paragraph (b) of this section, as specified in the airport security program. The airport operator shall maintain ASC training documentation in its

principal operations office until 180 days after the termination of each individual serving as an ASC.

(d) With respect to training required under this section, whenever a person completes recurrent training in the calendar month before or the calendar month after the calendar month in which that training is required, that person is considered to have completed the training in the calendar month in which it was required.

§ 107.7 Inspection authority.

(a) Each airport operator shall allow the Administrator, including FAA Special Agents, at any time or place, to make any inspections or tests to determine compliance of the airport operator, air carrier, foreign air carrier, and other airport tenants with -

(1) the airport security program;

(2) this part;

(3) 49 CFR part 175, which relates to the carriage of hazardous materials by aircraft; and

(4) 49 U.S.C. Subtitle VII, as amended.

(b) At the request of the Administrator, each airport operator shall provide evidence of compliance with this part and its airport security program.

(c) On request of any FAA Special Agent, and presentation of valid FAA-issued credentials, each airport operator shall issue to that agent access and identification media to provide the special agent with unescorted access to, and movement within, critical security areas and restricted operations areas.

§ 107.9 Falsification.

No person may make, or cause to be made, any of the following:

(a) Any fraudulent or intentionally false statement in any application for any security program, access medium, or identification medium, or any amendment thereto, under this part.

(b) Any fraudulent or intentionally false entry in any record or report that is kept, made, or used to show compliance with this part, or exercise any privileges under this part.

(c) Any reproduction or alteration, for fraudulent purpose, of any report, record, security program, access medium, or identification medium issued under this part.

§ 107.11 Security responsibilities of persons.

(a) No person may:

(1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause a person to tamper or interfere with, compromise, modify, or circumvent, any security system, method, or procedure implemented under this part.

(2) Enter, or be present within, a critical security area or restricted operations area without complying with the systems, methods, or procedures being applied to control access to, or presence in, such areas.

(3) Use, allow to be used, or cause to be used, any airport-approved access medium or identification medium that authorizes the access or presence of persons and vehicles in critical security areas or restricted operations areas in any other manner than that for which it was issued by the appropriate authority under this part, part 108, or part 129 of this chapter.

(b) Except as provided in 49 U.S.C. Subtitle VII, and paragraphs (c) and (d) of this section, no individual may have any deadly or dangerous weapon, explosive, incendiary, or other destructive substance on or about the individual's person or accessible property when entering, or within, a critical security area or restricted operations area of an airport governed by this part, or a sterile area governed under § 108.201 of this chapter.

(c) The provisions of this section with regard to paragraphs (a) and (b) of this section do not apply to persons authorized by the Federal government, airport operator, air carrier, or foreign air carrier to conduct inspections for compliance with this part, part 108, or part 129 of this chapter, or 49 U.S.C. Subtitle VII, while they are conducting an inspection.

(d) The provisions of this section with respect to firearms and weapons do not apply to the following:

(1) Law enforcement personnel required to carry a firearm or other weapon while in the performance of their duties at the airport .

(2) Persons authorized to carry a firearm under § 108.213, § 108.215, or § 129.27 of this chapter.

(3) Persons authorized to carry a firearm in a sterile area, critical security area, or restricted operations area under this part, an approved airport security program, an approved air carrier security program, or a security program used in accordance with § 129.25 of this chapter.

(4) Properly declared firearms in checked baggage for transport under § 108.213 of this chapter.

(5) Transportation of hazardous materials under 49 CFR part 175.

(6) Federal Air Marshals.

(7) Aircraft operators not subject to part 108 or part 129 of this chapter carrying firearms in accordance with state and local law.

Subpart B - Airport security program.

§ 107.101 General requirements.

(a) No person may operate an airport subject to this part unless it adopts and carries out an airport security program that -

(1) Provides for the safety and security of persons and property on an aircraft operating in air transportation or intrastate air transportation against an act of criminal violence, aircraft piracy, and the introduction of deadly or dangerous weapon, explosive, incendiary, or other destructive substance onto an aircraft;

(2) Is in writing and is signed by the airport operator or any person to whom the airport operator has delegated authority in this matter;

(3) Includes the items listed in § 107.103 of this part;

(4) Is organized in the same sequence as § 107.103 of this part to the extent practicable; and

(5) Has been approved by the Administrator.

(b) The airport operator shall maintain one complete copy of the security program in its principal operations office, and make it available for inspection upon the request of the Administrator.

(c) Each airport operator shall -

(1) Restrict the distribution, disclosure, and availability of sensitive security information, as defined in part 191 of this chapter, to persons with a need to know; and

(2) Refer all requests for sensitive security information by other persons to the Administrator.

§ 107.103 Content.

(a) Except as otherwise approved by the Administrator, each airport regularly serving an air carrier, or foreign air carrier, required to conduct screening under § 108.101(a)(1) or § 129.25(b)(1) of this chapter, shall include in the security program a description of the following -

(1) Name, means of contact, duties, and training requirements of the airport security coordinator, and designated alternates, required under § 107.5 of this part.

(2) Security compliance program that specifies procedures the airport operator will implement to ensure persons with authorized unescorted access to critical security areas and restricted operations areas comply with 107.9 and § 107.11 (a) and (b) of this part, including revocation of unescorted access authority of persons that fail to comply with security requirements.

(3) Critical security areas, including -

(i) Dimensions and a map detailing boundaries and pertinent features;

(ii) Each activity or entity on, or adjacent to, a critical security area that affects security;

(iii) Procedures, facilities, and equipment used to perform the access control functions required under § 107.201(b)(1) of this part; and

(iv) Notification signs required under § 107.201(b)(7) of this part.

(4) Restricted operations areas, including -

(i) Dimensions and a map detailing boundaries, and pertinent features;

(ii) Each activity or entity on, or adjacent to, a restricted operations area that affects security;

(iii) Procedures, facilities, and equipment used to perform the access control functions required under §107.203(b)(1) of this part; and

(iv) Notification signs required under § 107.203(b)(7) of this part.

(5) Sterile areas, including -

(i) Dimensions and a map detailing boundaries and pertinent features;

(ii) Activities and tenants located within the sterile area;

(iii) Access controls to be used when the passenger-screening checkpoint is non-operational and the entity responsible for that access control; and

(iv) Procedures, facilities, and equipment used to control access as specified in §107.205 of this part.

(6) Access investigation procedures used to comply with § 107.207 of this part.

(7) Personnel and vehicle identification systems as described in § 107.209 of this part.

(8) Escort procedures in accordance with §107.205(d) of this part.

(9) Challenge procedures in accordance with § 107.209(f) of this part.

(10) Training programs required under § 107.211 and § 107.215 of this part.

(11) Law enforcement support used to comply with § 107.213(a) of this part.

(12) System for maintaining records and schedule for reporting records, as described in § 107.219 of this part.

(13) Procedures, facilities, and equipment used to support air carrier or foreign air carrier screening functions of §108.211 of this chapter.

(14) Procedures, facilities, and equipment incorporated in the contingency plan required under § 107.301 of this part.

(15) Procedures for the distribution, storage, and disposal of Security Directives, Information Circulars, and, as appropriate, classified information, as specified in § 107.303 of this part.

(16) Procedures for public advisories as specified in § 107.305 of this part.

(17) Incident management procedures used to comply with § 107.307 of this part.

(18) Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters and other emergencies or unusual conditions.

(19) Each exclusive area required under § 107.111 of this part.

(20) Each airport tenant security program as specified in §107.113 of this part.

(b) Except as otherwise approved by the Administrator, each airport regularly serving an air carrier or foreign air carrier required to conduct screening under § 108.101(a)(2) or (a)(3), and § 129.25(b)(2) or (b)(3) of this chapter shall include in the security program a description of the following -

(1) Name, means of contact, duties, and training requirements of the airport security coordinator, and designated alternates, as required under § 107.5 of this part;

(2) Law enforcement support used to comply with § 107.213(a) of this part;

(3) Training program for law enforcement personnel required under § 107.215 of this part;

(4) System for maintaining records and schedule for reporting records, as described in § 107.219 of this part;

(5) Procedures, facilities, and equipment incorporated in the contingency plan required under § 107.301 of this part;

(6) Procedures for the distribution, storage, and disposal of Security Directives, Information Circulars, and, as appropriate, classified information, as specified in § 107.303 of this part;

(7) Procedures for public advisories as specified in § 107.305 of this part; and

(8) Incident management procedures used to comply with § 107.307 of this part.

(c) Except as otherwise approved by the Administrator, each airport regularly serving an air carrier or foreign air carrier required to have a security program under § 108.101 (a)(4) or § 129.25(b) (4) of this chapter, shall include in the security program a description of the following--

(1) Name, means of contact, duties, and training requirements of the airport security coordinator, and designated alternates, required under § 107.5 of this part;

(2) Law enforcement support used to comply with § 107.213(b) of this part;

(3) Training programs for law enforcement personnel required under § 107.215 of this part;

(4) System for maintaining records and schedule for reporting records, as described in § 107.219 of this part;

(5) Procedures for the distribution, storage, and disposal of Security Directives, Information Circulars, and, as appropriate, classified information, as specified in § 107.303 of this part;

(6) Procedures for public advisories as specified in § 107.305 of this part; and

(7) Incident management procedures used to comply with § 107.307 of this part.

(d) The airport operator may comply with paragraphs (a), (b), and (c) of this section by including in the security program, as an appendix, any document that contains the information

required by paragraphs (a), (b), and (c). Such an appendix shall be referenced in the corresponding section(s) of the security program.

§ 107.105 Approval and amendments.

(a) Approval of security program. Unless otherwise authorized by the Assistant Administrator, each airport operator required to have an airport security program under this part shall submit its proposed airport security program to the Assistant Administrator for approval at least 90 days before any air carrier or foreign air carrier, required to have a security program under § 108.101 or § 129.25 of this chapter, is expected to begin operations. Such requests shall be processed as follows:

(1) Within 30 days after receiving the proposed airport security program, the Assistant Administrator will either approve the program or give the airport operator written notice to modify the program to comply with the applicable requirements of this part.

(2) Within 30 days of receiving a notice to modify, the airport operator may either submit a modified security program to the Assistant Administrator for approval, or petition the Administrator to reconsider the notice to modify. A petition for reconsideration must be filed with the Assistant Administrator. Except in the case of an emergency requiring immediate action in the interest of safety, the filing of the petition stays the notice pending a decision by the Administrator.

(3) Upon receipt of a petition for reconsideration, the Assistant Administrator either amends or withdraws the notice, or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the Assistant Administrator to withdraw or amend the notice to modify, or by affirming the notice to modify.

(b) Amendment Requested by an Airport Operator. Except as provided in § 107.107 (c) of this part, an airport operator may submit a request to the Assistant Administrator to amend its airport security program, as follows:

(1) The application must be filed with the Assistant Administrator at least 45 days before the date it proposes for the amendment to become effective, unless a shorter period is allowed by the Assistant Administrator. However, in accordance with the procedures in this paragraph, it may take longer than 45 days for a final decision by the Administrator.

(2) Within 30 days after receiving a proposed amendment, the Assistant Administrator, in writing, either approves or denies the request to amend.

(3) An amendment to an airport security program may be approved if the Assistant Administrator determines that safety and the public interest will allow it, and the proposed amendment provides the level of security required under this part.

(4) Within 30 days after receiving a denial, the airport operator may petition the Administrator to reconsider the denial.

(5) Upon receipt of a petition for reconsideration, the Assistant Administrator either approves the request to amend or transmits the petition, together with any pertinent information, to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the Assistant Administrator to approve the amendment or affirm the denial.

(c) Amendment by the FAA. If safety and the public interest require an amendment, the Assistant Administrator may amend an airport security program as follows:

(1) The Assistant Administrator sends to the airport operator a notice, in writing, of the proposed amendment, fixing a period of not less than 30 days within which the airport operator may submit written information, views, and arguments on the amendment.

(2) After considering all relevant material, the Assistant Administrator notifies the airport operator of any amendment adopted or rescinds the notice. If the amendment is adopted, it becomes effective not less than 30 days after the airport operator receives the notice of amendment, unless the airport operator petitions the Administrator to reconsider no later than 15 days before the effective date of the amendment. The airport operator shall send the petition for reconsideration to the Assistant Administrator. A timely petition for reconsideration stays the effective date of the amendment.

(3) Upon receipt of a petition for reconsideration, the Assistant Administrator either amends or withdraws the notice, or transmits the petition, together with any pertinent information

to the Administrator for reconsideration. The Administrator disposes of the petition within 30 days of receipt by either directing the Assistant Administrator to withdraw or amend the amendment, or by affirming the amendment.

(d) Emergency Amendments. Notwithstanding paragraphs (a), (b), and (c) of this section, if the Assistant Administrator finds that there is an emergency requiring immediate action with respect to safety in air transportation or in air commerce that makes procedures in this section contrary to the public interest, the Assistant Administrator may issue an amendment, effective without stay, on the date the airport operator receives notice of it. In such a case, the Assistant Administrator shall incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The airport may file a petition for reconsideration under paragraph (c) of this section, however, this does not stay the effectiveness of the emergency amendment.

§ 107.107 Changed conditions affecting security.

(a) After approval of the airport security program, each airport operator shall notify the Administrator when changes have occurred to the -

(1) Procedures, methods, system, facilities, training, equipment, area descriptions, staffing, or any other description or requirement prescribed by the airport security program;

(2) Nature of air carrier or foreign air carrier operations, including changes to level of service, aircraft, and leasehold; or

(3) Layout or physical structure of any area under the control of the airport operator, air carrier, or foreign air carrier used to support the screening, access, or movement control functions required under parts 107, 108, or 129 of this chapter.

(b) Whenever a changed condition described in paragraph (a) of this section occurs, each airport operator shall notify the Administrator within 2 hours, or within the time specified in its security program, of discovery of the changed condition and each interim measure being taken to maintain adequate security until an appropriate amendment to the security program is approved. Each interim measure(s) must be acceptable to the Administrator.

(c) For changed conditions under 60 days duration, each airport operator shall forward the information required in paragraph (b) of this section in writing to the Administrator within 72 hours of the original notification of the change condition(s). The Administrator will notify the airport operator of the disposition of the notification in writing. If approved by the Administrator, this written notification will become a part of the airport security program for the duration of the changed condition(s).

(d) For changed conditions over 60 days duration, each airport operator shall forward the information required in paragraph (b) of this section in the form of a proposed amendment to the airport operator's security program, as required under § 107.105 of this part. The request for

an amendment shall be made within 30 days of the discovery of the changed condition(s). The Administrator will respond to the request in accordance with § 107.105 of this part.

§ 107.109 Alternate Means of Compliance.

If the safety and security of the airport, and air carrier passengers and operations, are not diminished, the Administrator may approve an airport security program that permits the use of alternate means of compliance with the requirements of this part. Such an amendment may be considered for an airport operator of an airport that is served seasonally or infrequently by an air carrier or foreign air carrier required to conduct screening under § 108.101(a)(1) or § 129.25(b)(1) of this chapter.

§ 107.111 Exclusive area agreements.

(a) The Administrator may approve an amendment to an airport security program in accordance with this section that permits an air carrier or foreign air carrier that has an approved security program under part 108 or part 129 to assume responsibility for specified security measures for all or portions of the critical security areas or restricted operations areas. The assumption of responsibility must be exclusive to one air carrier or foreign air carrier, and shared responsibility among air carriers or foreign air carriers is not permitted.

(b) An exclusive area agreement shall be in writing and maintained in the airport security program. This agreement shall contain descriptions of the following:

(1) Dimensions, boundaries, and pertinent features of each area, or individual access points, over which the air carrier or foreign air carrier will exercise exclusive security responsibility.

(2) Procedures and a description of the facilities and equipment used to perform the control functions described in § 107.201 or § 107.203 of this part, as appropriate.

(3) Procedures by which the air carrier or foreign air carrier will immediately notify the airport operator and provide for alternative security measures when the procedures, facilities, and equipment required by the agreement are not adequate to perform the control functions in accordance with § 107.201 or § 107.203 of this part, as appropriate.

(4) Methods by which the airport operator will monitor and audit the air carrier’s or foreign air carrier's compliance with the exclusive area agreement.

(5) Circumstances under which the airport operator will terminate the exclusive area agreement for cause and resume responsibility for security measures covered by the exclusive area agreement.

§ 107.113 Airport tenant security programs.

(a) The Administrator may approve an airport tenant security program that permits an airport tenant having access to a critical security area or restricted operations area to accept responsibility for all or part of the specified security measures of §§ 107.201 or 107.203 of this

part within the tenant’s leased areas or areas designated for the tenant’s exclusive use under an agreement with the airport operator. This airport tenant security program shall be included in the airport security program.

(b) The airport tenant security program shall include the following:

(1) Dimensions, boundaries, and pertinent features of each area covered by the airport tenant security program.

(2) Measures by which the tenant will carry out within its designated areas the security requirements imposed by the Administrator on the airport operator.

(3) Methods by which the airport operator will monitor and audit the tenant's compliance with the security requirements.

(4) Terms of the agreement, including monetary and other penalties, to which the tenant may be subject if it fails to carry out any security requirements it agreed to perform.

(5) Circumstances under which the airport operator will terminate the airport tenant security program for cause.

(c) The airport operator may not be found to be in violation of a requirement of this part in any case in which the airport operator demonstrates that:

(1) The tenant, or an employee, permittee, or invitee of the tenant, is responsible for such violation; and

(2) The airport operator has complied with all measures in its airport security program to ensure the tenant has complied with the airport tenant security program.

(d) The Administrator may amend or terminate an airport tenant security program in accordance with § 107.105 of this part.

Subpart C - Operations

§ 107.201 Security of the critical security area.

(a) Each airport operator required to have an airport security program under § 107.103 (a) of this part shall establish at least one critical security area and describe each critical security area in its security program.

(b) Each airport operator required to establish a critical security area shall do the following:

(1) Prevent the entry of unauthorized individuals and ground vehicles by establishing and carrying out a system, method, or procedure for controlling access to critical security areas of the airport in accordance with § 107.205 of this part.

(2) Establish and carry out a personnel and vehicle identification system described under § 107.209 of this part to control the presence and movement of persons and ground vehicles within the critical security area.

(3) Establish and use escort procedures in accordance with § 107.205(d) of this part.

(4) Establish and use challenge procedures required under § 107.209(f) of this part.

(5) Subject each individual to a personnel background check as described in § 107.207 of this part before authorizing unescorted access to a critical security area.

(6) Train each individual before granting unescorted access to the critical security area, as required in § 107.211(b) of this part.

(7) Post signs at critical security area access points and on the perimeter that provide warning of the prohibition against unauthorized access. Such warning signs shall be posted by each airport operator not later than 2 years after [the effective date of this rule].

§ 107.203 Security of the restricted operations area.

(a) For those portions of the airport where air carrier and foreign air carrier aircraft take off, land, taxi, park and otherwise maneuver but are not delineated as a critical security area, each airport operator required to have an airport security program under § 107.103(a) of this part shall establish and describe in its security program a restricted operations area.

(b) Each airport operator required to establish a restricted operations area shall do the following:

(1) Use a system, method, or procedure for controlling access to restricted operations areas of the airport in accordance with § 107.205(b) of this part.

(2) Subject each individual to a 5-year employment history verification before authorizing unescorted access to the restricted operations area.

(3) Establish and use a personnel and vehicle identification system described under § 107.209 of this part to control the presence and movement of individuals and ground vehicles within the restricted operations area.

(4) Establish and use escort procedures in accordance with § 107.205(d) of this part.

(5) Establish and use challenge procedures required under § 107.209(f) of this part.

(6) Provide security information as described in § 107.211(c) of this part to each individual with unescorted access to the restricted operations area.

(7) Post signs on restricted operations area access points and perimeters that provide warning of the prohibition against unauthorized access. Signs shall be implemented by each airport operator not later than 2 years after [the effective date of this rule].

§ 107.205 Access control systems.

(a) Critical Security Area. Except as provided in paragraph (g) of this section, the system, method, or procedure for controlling access to the critical security area required under § 107.201 (b)(1) of this part shall--

(1) Ensure that only those individuals authorized to have unescorted access to the critical security area are able to obtain that access;

(2) Ensure that an individual is immediately denied access to a critical security area when that person’s access authority for that area is withdrawn;

(3) Provide a means to differentiate between individuals authorized to have access to an entire critical security area and individuals authorized access to only a particular portion of a critical security area; and

(4) Be capable of limiting an individual's access to a critical security area by time and date, as specified in the airport contingency plan required under §107.301 of this part.

(b) Restricted Operations Area. Except as provided in paragraphs (c) and (e) of this section, the system, method, or procedure for controlling access to the restricted operations area required under § 107.203 (b)(1) of this part shall--

(1) Prevent the entry of unauthorized individuals and ground vehicles;

(2) Provide for detection of and response to each unauthorized presence in or access or attempted access to, the restricted operations area by an individual whose entry is not authorized in accordance with the airport security program;

(3) Be locally controlled; and

(4) Incorporate accountability procedures to maintain the integrity of that system, method, or procedure.

(c) Secondary access media. An airport operator may issue a second access medium to individuals authorized access to critical security areas and restricted operations areas, if the airport operator follows methods and procedures in the airport security program that--

(1) Verify the access authorization of the individuals granted unescorted access to critical security areas and restricted operations areas but are not in possession of their original access medium;

(2) Limit time of access with second access medium;

(3) Retrieve the second access medium when expired; and

(4) Deactivate or invalidate temporarily the original access medium until the time that the individual returns the second access medium.

(d) Escorting. Each airport operator shall establish and implement procedures for escorting individuals who do not have unescorted access authority to a critical security area or a restricted operations area that -

(1) Ensure that only individuals with unescorted access authority are permitted to escort;

(2) Ensure that the escorted individuals are continuously accompanied or supervised in a manner sufficient to take action should escorted individuals engage in activities other than those for which escorted access was granted;

(3) Identify what action is to be taken by the escort, or other authorized individual, should individuals under escort engage in activities other than those for which access was granted;

(4) Prescribe law enforcement support of escort activities; and

(5) Ensure that individuals escorted to a sterile area without being screened under § 108.201 of this chapter remain under escort in accordance with this section, or submit to screening pursuant to § 108.201 of this part.

(e) Group validation. An airport operator may submit for approval by the Administrator procedures in its airport security program for group validation without each individual validating access authority at individual access points.

(f) Sterile areas. With the exception of access points leading from a critical security area, each airport operator shall ensure that all points that provide access to the sterile area from nonpublic areas meet the requirements of this section.

(g) Alternative systems. The Administrator may approve an amendment to an airport security program that provides an alternative system, method, or procedure that provides an overall level of security equal to that which would be provided by the system, method, or procedure described in paragraphs (a) and (b) of this section.

§ 107.207 Employment history, verification, and criminal history records checks. [Reserved]

(Note: There is a separate rulemaking action that will result in new text for this section. To avoid confusion, the section is not repeated here. See the preamble for further explanation.)

§ 107.209 Identification systems.

(a) Personnel identification system. The personnel identification system under §§ 107.201(b)(2) or 107.203(b)(3) of this part shall include the following:

(1) Personnel identification media that -

(i) Convey accurate identification of the individual to whom the identification medium is issued;

(ii) Indicate clearly the scope of the individual's access and movement privileges;

(iii) Indicate clearly an expiration date; and

(iv) Are of sufficient size and appearance as to be readily observable for challenge purposes.

(2) Procedures to ensure that each individual continuously displays the identification medium issued to that individual.

(3) Procedures to ensure accountability through the following -

(i) Retrieving expired identification media;

(ii) Reporting lost or stolen identification media;

(iii) Securing unissued identification media stock and supplies;

(iv) Auditing the system at a minimum of once a year or sooner as necessary to ensure the integrity and accountability of all identification media;

(v) As specified in the airport security program, revalidate the identification system or reissue identification media if a portion of all issued identification media become unaccounted for, including identification media that is combined with access media; and

(vi) Ensure that only one identification medium is issued to an individual at a time. A replacement identification medium may only be issued if an individual declares in writing that the medium has been lost or stolen.

(b) Vehicle identification system. The vehicle identification system required under § 107.201(b)(2) and § 107.203(b)(3) of this part shall include the following:

(1) Vehicle identification media that -

(i) Indicate clearly the scope of the vehicle's access and movement;

(ii) Indicate clearly an expiration date; and

(iii) Are of sufficient size and appearance as to be readily visible when affixed to the vehicle.

(2) Procedures to ensure accountability through-

(i) Retrieving expired vehicle identification media;

(ii) Reporting lost or stolen vehicle media;

(iii) Securing unissued vehicle identification media stock and supplies;

(iv) Auditing the system at a minimum of once a year or sooner as necessary to ensure accountability of all vehicle identification media;

(v) As specified in the airport security program, revalidate, or reissue vehicle identification media, if a portion of all issued vehicle identification media become unaccounted for; and

(vi) Ensure that only one identification medium is issued to a vehicle at a time. A replacement identification medium may only be issued if the owner of the vehicle, or designee, declares in writing that the medium has been lost or stolen.

(c) Part 139, Ground vehicle system. If approved by the Administrator, a vehicle access control and operations system may be used to meet the requirements of both § 139.329, Ground Vehicles and this section.

(d) Temporary identification media. Each airport operator shall issue personnel and vehicle identification media to persons whose duties are expected to be temporary. Temporary identification media system shall include procedures and methods to -

(1) Retrieve temporary identification media;

(2) Authorize the use of a temporary media for a limited time only; and

(3) Ensure that temporary media are distinct and clearly display an expiration date.

(e) Airport-approved identification media. The Administrator may approve the use of identification media meeting the criteria of this section that are issued by entities other than the airport operator, as described in the airport security program.

(f) Challenge program. Each airport operator shall establish and carry out a challenge program that requires each individual authorized unescorted access to critical security areas and restricted operations areas to ascertain the authority of any individual not displaying an authorized identification media to be present in such areas. A challenge program shall include procedures to verbally challenge or report individuals not visibly displaying authorized identification media that -

(1) Apply uniformly in both critical security areas and restricted operations areas, including exclusive areas;

(2) Identify how to challenge directly or report individuals not visibly displaying authorized identification medium, including procedures to notify the appropriate authority; and

(3) Prescribe law enforcement support of challenge procedures, including response to reports of individuals not displaying authorized identification.

(g) Effective date. The identification systems described in this section shall be implemented by each airport operator not later than 2 years after [insert the effective date of this rule].

§ **107.211 Training.**

(a) Each airport operator shall ensure that individuals performing security-related functions for the airport operator are briefed on the provisions of this part, applicable Security Directives and Information Circulars promulgated pursuant to § 107.303 of this part, and the airport security program, to the extent that such individuals need to know in order to perform their duties.

(b) An airport operator may not authorize any individual unescorted access to the critical security area unless that individual has successfully completed training in accordance with the FAA-approved curriculum specified in the security program. This curriculum must detail the methods of instruction and include at least the following topics -

(1) Control, use, and display of airport-approved access and identification media;

(2) Escort and challenge procedures, and the law enforcement support for these procedures;

(3) Security responsibilities as specified in § 107.9 and § 107.11 (a) and (b) of this part; and

(4) Any other topics specified in the airport security program.

(c) An airport operator may not authorize any individual unescorted access to a restricted operations area unless that individual has been provided, and so acknowledges in writing, information in accordance with the airport security program, including -

(1) Control, use, and display of airport-approved access and identification media;

(2) Escort and challenge procedures and the law enforcement support for these procedures;

(3) Security responsibilities as specified in § 107.9 and § 107.11 (a) and (b) of this part; and

(4) Any other topics specified in the airport security program.

(d) Each airport operator shall maintain a record of all training given to each individual under this section and written acknowledgment required under paragraph (c) of this section, for 180 days after the termination of that person's unescorted access authority.

(e) Training described in this section shall be implemented by each airport operator not later than 2 years after [insert the effective date of this rule].

§ 107.213 Law enforcement support.

(a) In accordance with § 107.215 of this part, each airport operator required to have an airport security program under § 107.103(a) and (b) of this part shall provide:

(1) Law enforcement personnel in the number and manner adequate to support its security program.

(2) Uniformed law enforcement personnel in the number and manner adequate to support each passenger-screening system required under § 108.201 or § 129.25 of this chapter.

(b) Each airport required to have an airport security program under § 107.103(c) of this part shall ensure that:

(1) Law enforcement personnel are available and committed to respond to an incident at the request of an air carrier or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter.

(2) The procedures by which to request law enforcement support are provided to each air carrier or foreign air carrier that has a security program under part 108 or § 129.25 of this chapter.

§ 107.215 Law enforcement personnel.

(a) Each airport operator shall ensure that law enforcement personnel used to meet the requirements of § 107.213 of this part, meet the following qualifications while on duty at the airport--

(1) Have arrest authority described in paragraph (b) of this section;

(2) Are identifiable by appropriate indicia of authority;

(3) Are armed with a firearm and authorized to use it; and

(4) Have completed a training program that meets the requirements of paragraphs (c) and (d) of this section.

(b) Each airport operator shall ensure that law enforcement personnel used to meet the requirements of § 107.213 of this part have the authority to arrest, with or without a warrant, while on duty at the airport for the following violations of the criminal laws of the State and local jurisdictions in which the airport is located--

(1) A crime committed in the presence of the law enforcement personnel; and

(2) A felony, when the law enforcement personnel has reason to believe that the suspect has committed it.

(c) The training program required by paragraph (a)(4) of this section shall--

(1) In the case of Law Enforcement Officers, meet the training standards prescribed by either the State or local jurisdiction in which the airport is located for law enforcement personnel performing comparable functions.

(2) In the case of private Law Enforcement Personnel, be trained in a manner acceptable to the Administrator, if the State and local jurisdictions in which the airport is located do not prescribe training standards for private security personnel who meet the standards in paragraph (a) of this section.

(3) Include training in -

(i) The use of firearms;

(ii) The courteous and efficient treatment of persons subject to inspection, detention, search, arrest, and other aviation security activities;

(iii) The responsibilities of law enforcement personnel under the airport security program; and

(iv) Any other subject the Administrator determines is necessary.

(d) Each airport operator shall document the training program required by paragraph (a)(4) of this section and--

(1) Maintain documentation of training in its principal operations office until 180 days after the departure or removal of each law enforcement personnel from service at the airport; and

(2) Make training documentation available for inspection upon the request of the Administrator.

§ 107.217 Supplementing law enforcement personnel.

(a) When the Administrator decides, after being notified by an airport operator as prescribed in this section, that not enough qualified State, local, and private law enforcement personnel are available to carry out the requirements of § 107.213 of this part, the Administrator may authorize the airport operator to use, on a reimbursable basis, personnel employed by the Administrator, or by another department, agency, or instrumentality of the Government with the consent of the head of the department, agency, or instrumentality, to supplement State, local, and private law enforcement personnel.

(b) Each request for the use of Federal personnel must be submitted to the Administrator and include the following information:

(1) The number of passengers enplaned at the airport during the preceding calendar year and the current calendar year as of the date of the request.

(2) The anticipated risk of criminal violence, sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.

(3) A copy of that portion of the airport security program which describes the law enforcement support necessary to comply with § 107.213 of this part.

(4) The availability of law enforcement personnel who meet the requirements of § 107.215 of this part, including a description of the airport operator's efforts to obtain law enforcement support from State, local, and private agencies and the responses of those agencies.

(5) The airport operator's estimate of the number of Federal personnel needed to supplement available law enforcement personnel and the period of time for which they are needed.

(6) A statement acknowledging responsibility for providing reimbursement for the cost of providing Federal personnel.

(7) Any other information the Administrator considers necessary.

(c) In response to a request submitted in accordance with this section, the Administrator may authorize, on a reimbursable basis, the use of personnel employed by a Federal agency, with the consent of the head of that agency.

§ 107.219 Records.

(a) All records required to be maintained under this part shall be furnished to the Administrator pursuant to the schedule included in the airport security program.

(b) Each airport operator shall ensure that -

(1) A record is made of each law enforcement response taken in furtherance of this part; and

(2) The record is maintained for a minimum of 180 days.

(c) Data developed in response to paragraph (b) of this section must include at least the following:

(1) The number and type of deadly or dangerous weapon, explosive, incendiary, or other destructive substance discovered during any passenger-screening process, and the method of detection of each;

(2) The number of acts and attempted acts of aircraft piracy.

(3) The number of bomb threats received, real and simulated bombs found, and actual detonations on the airport.

(4) The number of detentions and arrests, including -

(i) Name, address, and the immediate disposition of each individual detained or arrested;

(ii) Type of deadly or dangerous weapon, explosive, incendiary, or other destructive substance confiscated, as appropriate; and

(iii) Identification of the air carriers or foreign air carriers on which the individual detained or arrested was, or was scheduled to be, a passenger, or which screened that individual, as appropriate.

(d) Each airport operator required to have an airport security program under § 107.103 (a) of this part shall make, and maintain for 180 days, records of corrective action imposed on persons that fail to comply with § 107.9 and § 107.11 (a) and (b) of this part.

(e) Each airport operator shall make and maintain any additional records required by the Administrator, this part, and the airport security program, including, but not limited to, the following recordkeeping requirements of this part:

(1) § 107.5, Airport security coordinator.

(2) § 107.207, Employment verification.

(3) § 107.211, Training.

(4) § 107.215, Law enforcement personnel.

Subpart D - Contingency Measures.

§ 107.301 Contingency plan.

Each airport operator required to have a security program under § 107.103(a) and (b) of this part shall adopt a contingency plan and shall:

(a) Implement its contingency plan when directed by the Administrator.

(b) Conduct reviews and exercises of its contingency plan with all air carriers and foreign air carriers and all persons having responsibilities under the plan to ensure that all parties involved know their responsibilities and that all information contained in the plan is current.

§ 107.303 Security Directives and Information Circulars.

(a) When a threat against civil aviation becomes known, the Assistant Administrator may issue an information circular to notify airport operators of the general situation or a Security Directive setting forth mandatory countermeasures to an assessed threat.

(b) Each airport operator required to have an airport security program shall comply with each Security Directive issued to the airport operator by the Administrator, within the time prescribed in the Security Directive for compliance.

(c) Each airport operator that receives a Security Directive shall -

(1) Immediately upon receipt from the FAA, or within the time prescribed in the Security Directive, verbally acknowledge receipt of the Security Directive to the FAA, followed by written acknowledgment of receipt within 24 hours;

(2) Not later than 72 hours after delivery by the FAA, or within the time prescribed in the Security Directive, specify the method by which the measures in the Security Directive have been implemented (or will be implemented, if the Security Directive is not yet effective) by providing the FAA a copy of the written measures and implementation procedures; and

(3) Ensure that information regarding the Security Directive and measures implemented in response to the Security Directive are distributed to specified personnel, as prescribed in the Security Directive, and to other personnel with an operational need to know.

(d) In the event that the airport operator is unable to implement paragraph (b)(2) of this section, the airport operator shall submit, within 72 hours after receipt of the Security Directive, proposed alternative measures and the basis for submitting the alternative measures to the Administrator for approval. Within 48 hours after receiving the airport operator's proposed alternative measures, the Administrator either approves the proposed alternative countermeasures or notifies the airport operator to modify the alternative countermeasures to comply with the requirements of the Security Directive. The airport operator shall implement any alternative measures approved by the Administrator within 72 hours of receipt of notification of the Administrator's determination.

(e) Each airport operator that receives a Security Directive or Information Circular and each person who receives information from a Security Directive or Information Circular shall:

(1) Restrict the availability of the Security Directive or Information Circular, and information contained in either document, to those persons with an operational need to know.

(2) Refuse to release the Security Directive or Information Circular, and information contained in either document, to persons other than those who have an operational need-to-know without the prior written consent of the Administrator.

(f) The airport security coordinator, or an individual designated by the airport operator, may receive classified information related to national security if the airport security coordinator, or designee, has applied to the Administrator and received the appropriate security clearances.

§ 107.305 Public advisories.

When advised by the Administrator, each airport operator shall prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures. Such information shall be posted in the manner and for the timeframe specified in the airport security program.

§ 107.307 Incident management.

(a) As described in the airport security program, each airport operator shall establish procedures to evaluate the appropriate response to threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations, including bomb threats.

(b) Immediately upon receipt of a threat of any of the incidents described in paragraph (a), each airport operator shall -

(1) Evaluate the threat in accordance with its airport security program;

(2) Initiate appropriate action as specified in the Airport Emergency Plan under §139.325 of this chapter; and

(3) Immediately notify the Administrator of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.

(c) Airport operators required to have an airport security program under §107.103(c) of this part but not subject to part 139 of this chapter, Certification and Operations: Land Airports Serving Certain Air Carriers, shall develop emergency response procedures to incidents of threats identified in paragraph (a).

(d) To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator shall review the procedures required in paragraphs (a) and (b) with all persons having responsibilities for such procedures.

Part 139 --Certification and Operations: Land Airports Serving Certain Air Carriers

2. The authority citation for part 139 continues to read as follows:

Authority: 49 U.S.C. 106 (g), 40113, 44701-44706, 44709, 44719.

3. Section 139.325 is amended by redesignating paragraph (h) as new paragraph (j) and adding new paragraphs (h) and (i) to read as follows:

§ 139.325 Airport emergency plan

*** * * * ***

(h) Each airport subject to part 107, Airport Security, shall ensure that instructions for response to paragraphs (b)(2) and (b)(6) of this section in the airport emergency plan are consistent with its approved airport security program.

(i) FAA Advisory Circulars in the 150 Series contain standards and procedures for the development of an airport emergency plan which are acceptable to the Administrator.

* * * * *

Anthony Fainberg

Director, Office of Civil Aviation Security Policy and Planning

Issued in Washington D.C on July 21, 1997.